Samenvatting

De gemeente Maastricht stelt het strategisch informatiebeveiligingsbeleid 3.0 vast. Hiermee wordt de informatiebeveiliging organisatiebreed geborgd. Onze digitale omgeving is kwetsbaar. Dit vraagt om extra inspanningen om de weerbaarheid op het gebied van informatieveiligheid te versterken en te borgen. De wet stelt dat we aan strenge eisen moeten voldoen. Het te behalen niveau betekent dat beheersmaatregelen zijn gedocumenteerd, gestructureerd en geformaliseerd worden uitgevoerd en dat de uitvoering aantoonbaar en toetsbaar is. De concrete uitwerking wordt opgenomen in het informatiebeveiligingsplan.

Beslispunten

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.

Besluit Burgemeester en wethouders d.d. 16 december 2025:

Conform.

1. Aanleiding

De Network and Information Security directive, of NIS2-richtlijn, is de opvolger van de NIS-richtlijn. Deze richtlijn is vastgesteld door de Europese Unie (EU) en bedoeld om de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. De NIS2-richtlijn vergroot de reikwijdte van de NIS-richtlijn door meer sectoren te omvatten, waaronder de (gemeentelijke) overheid. Ook stelt de richtlijn strengere beveiligingsnormen en meldingsvereisten voor incidenten. De NIS2-richtlijn wordt momenteel vertaald naar Nederlandse wetgeving in de vorm van de Cyberbeveiligingswet. In deze wetgeving zullen gemeentelijke overheden tot essentiële entiteit worden benoemd. De NIS2 verplichtingen worden onverkort overgenomen in de Nederlandse wetgeving. De Cyberbeveiligingswet treedt naar verwachting in de loop van 2026 in werking.

2. Beoogd effect

Het gemeentelijk informatiebeveiligingsbeleid in lijn brengen met de nieuwe wet- en regelgeving.

3. Argumenten

1.1 De richtlijn bevat een zorgplicht die organisaties verplicht 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. Vanuit de verschillende sectoren van NIS2 worden nadere regels gesteld aan de zorgplicht. Voor de overheid omvat dit in elk geval voldoen aan de Baseline Informatiebeveiliging Overheid (BIO) 2.0.

1.2 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), die hulp- en bijstand kan leveren. Factoren die een incident meldingswaardig maken, zijn bijvoorbeeld het aantal personen dat door de verstoring is geraakt, de tijdsduur van een verstoring en de mogelijke financiële verliezen. De drempelwaarden voor de overheid wordt verder uitgewerkt. Voor gemeenten is de Informatie Beveiliging Dienst (IBD) het Computer Security Incident Response Team.

1.3 Organisaties die onder de richtlijn vallen, krijgen ook verplicht toezicht. De NIS2-richtlijn schrijft voor dat een onafhankelijk toezichthouder (niet te verwarren met interbestuurlijk toezicht in het geval van medeoverheden) kijkt naar de naleving van de verplichtingen uit de richtlijn, zoals de zorg- en meldplicht. 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. Dit om mogelijke administratieve lasten van het toezicht tot een minimum te beperken. Voor gemeenten betekent dit dat de huidige verantwoording via de bestaande Eenduidige Normatiek Single Information Audit (ENSIA), al dan niet aangepast, blijft verlopen.

4. Kanttekeningen of risico's

1.1 Het niet tijdig voldoen aan NIS2- en Cyberbeveiligingswet-verplichtingen kan leiden tot sancties of reputatieschade.

5. Financiële gevolgen

Het vaststellen van dit strategisch Informatiebeveiligingsbeleid past binnen de bestaande begroting en kost geen extra geld. Aan de implementatie van eventuele (nieuwe) maatregelen voortvloeiend 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 bedrijfsvoering project portfolio. In dat geval vindt dekking plaats via het project, hetgeen ook een extra budgetaanvraag voor de begroting met zich mee kan brengen.

6. Vervolgtraject besluitvorming, uitvoering en evaluatie

De operationalisering van het strategisch informatiebeveiligingsbeleid, krijgt gestalte in de herziening van het tactisch informatiebeveiligingsbeleid; in het bedrijfsvoeringsportfolio project Invoering Cyberbeveiligingswet 2026 en de nieuwe gemeentebrede bewustwordingscampagne voor het personeel.
Door middel van GAP analyses BIO2.0 wordt geëvalueerd of vervolgprojecten nodig zijn.
De jaarlijkse awareness metingen geven in zicht in de stand van zaken rondom awareness.

7. Communicatie

Het strategisch informatiebeveiligingsbeleid wordt in het gemeenteblad bekendgemaakt en gepubliceerd via de openbare besluitenlijst van het College van B&W. Aan managers wordt het kenbaar gemaakt via de BMO groep op Stella en het zittend personeel kan kennis nemen via het

gemeentelijk intranet. Voor in dienst tredend nieuw personeel wordt het beleid opgenomen in de onboarding.