Gemeente Maastricht

GEMEENTEBLAD

Officiële uitgave van de gemeente Maastricht

Nr. 512145

18 november

2022

Strategisch informatiebeveiligingsbeleid

Gezien het voorstel van Burgemeester en Wethouders gemeente Maastricht d.d. 8 november 2022;

Besluit:
Vaststellen van het strategisch informatiebeveiligingsbeleid

Versiebeheer
Het beheer van dit document berust bij de Chief Information Security Officer (CISO) van de gemeente Maastricht.

Inleiding
Dit document beschrijft het strategische informatiebeveiligingsbeleid van de gemeente Maastricht voor de periode 2022-2025 en vervangt het in 2019 vastgestelde `Informatiebeveiligingsbeleid gemeente Maastricht'. Het voorgaande beleid was gebaseerd op de baseline informatiebeveiliging overheid versie 1.02. Dit nieuwe beleid is gebaseerd op de Visie Informatiebeveiliging en verwijst naar de baseline informatiebeveiliging overheid versie 1.04zv als het gaat om de concrete controls, maatregelen en handreikingen.

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, waaronder persoonsgegevens. Informatiebeveiliging gaat niet over ICT alleen, maar gaat over informatie in alle verschijningvormen binnen de organisatie. Informatiebeveiliging creëert daarmee waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de gemeentelijke organisatie.

Het strategisch informatiebeveiligingsbeleid van de gemeente Maastricht
De gemeente Maastricht baseert haar strategisch informatiebeveiligingsbeleid op de Visie Informatiebeveiliging, de Baseline Informatiebeveiliging Overheid en de 10 bestuurlijke principes voor informatiebeveiliging.

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 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.
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.

Baseline Informatiebeveiliging Overheid
Met ingang van 2020 is de baseline informatiebeveiliging overheid het vigerende normenkader voor de overheid (momenteel BIO-versie-1.04zv). De werkwijze van de BIO is gericht op risicomanagement. Dat wil zeggen dat de afdelingsmanagers nu meer moeten werken volgens de aanpak van de ISO 27001, de internationale norm voor informatiebeveiliging. Dit houdt voor het management in dat zij voortdurend keuzes en continue afwegingen moeten maken of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

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

10 Bestuurlijke principes voor informatiebeveiliging
De 10 bestuurlijke principes voor informatiebeveiliging zijn:
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.

Reikwijdte
De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen (zowel on-premise als SaaS), procesautomatisering, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategisch informatiebeveiligingsbeleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen (bijvoorbeeld DigiD, Suwinet, gemeentelijke basisregistraties, verplichte eisen van het Forum Standaardisatie etc.).
Het strategisch informatiebeveiligingsbeleid wordt, waar van toepassing, per onderwerp door zorg van het Directieteam (DT) aangevuld met specifieke beleidsdocumenten op tactisch niveau. Reeds door het DT vastgesteld tactisch beveiligingsbeleid blijft geldig.

Evaluatie en herziening strategisch informatiebeveiligingsbeleid
Het strategisch informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bij- en formeel vastgesteld.

Strategische doelen
De strategische doelen van het informatiebeveiligingsbeleid zijn:
- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- 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, Uitgangspunten en Richtlijnen strategisch informatiebeveiligingsbeleid
De gemeente Maastricht hanteert de onderstaande randvoorwaarden, uitgangspunten en richtlijnen voor het strategisch informatiebeveiligingsbeleid:
- Informatiebeveiliging maakt onderdeel uit van (contractuele) afspraken met ketenpartners;
- Bij het plaatsen van een informatiesysteem in de Cloud, is de inschrijver en eventuele onderaannemers ISO27001 (Informatiebeveiliging) gecertificeerd en/of is in het bezit van een geldige ISAE3402 SOC2 assurance rapportage en/of levert ten tijde van de inschrijving en jaarlijks een TPM-verklaring over de gehele dienstverlening inclusief onderaannemers, uitgegeven door een IT Auditor (RE en/of CISA), waarmee assurance wordt afgegeven over de kwaliteitsaspecten integriteit, beschikbaarheid en vertrouwelijkheid in opzet, bestaan en werking.
- Kennis over en bewustzijn van informatiebeveiliging onder medewerkers en het omgaan met persoonsgegevens wordt actief bevorderd en geborgd door het lijnmanagement in een doorlopende bewustwordingscampagne geïnitieerd door de chief information security officer (CISO) en de functionaris voor de gegevensbescherming (FG);
- De door het college van B&W gemandateerde verantwoordelijkheid voor informatiebeveiliging ligt bij de directeur bedrijfsvoering en dienstverlening;
- Het jaarlijks op te stellen (I&A) PORTFOLIO 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.

Informatiebeveiligingsorganisatie: Taken, Verantwoordelijkheden en Bevoegdheden
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 **Directieteam** stelt het tactisch informatiebeveiligingsbeleid en het I&A portfolio inclusief Informatiebeveilgingsopgaven vast.

De **Directeur bedrijfsvoering** is gemandateerd bevoegd en verantwoordelijk voor het waar nodig (laten) uitwerken, vaststellen en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op het strategisch informatiebeveiligingsbeleid;

Chief Information Security Officer
De gemeentelijke CISO heeft een onafhankelijk positie tegenover zowel het lijnmanagement als het bestuur van de gemeente.
De CISO is bevoegd en verantwoordelijk voor:
- Het opstellen, actualiseren en laten vaststellen van strategisch -, tactisch - en operationeel informatiebeveiligingsbeleid;
- Het opstellen en laten vaststellen van de Informatiebeveiligingsopgave in het I&A-portfolio;
- Het rapporteren over de uitvoering en voortgang van de Informatiebeveiligingsopgave aan de Directeur bedrijfsvoering/CIO en het Directieteam;
- Het geven van gevraagd en ongevraagd advies aan het bestuur en het management van de organisatie over te nemen maatregelen.

Specialist informatiebeveiliging
- Geeft uitvoering aan de Informatiebeveiligingsopgave;
- Identificeert en analyseert beveiligingsrisico's en formuleert verbetervoorstellen;
- Ondersteund het lijnmanagement bij informatiebeveiligingsvraagstukken;
- Adviseert de CISO over tactisch informatiebeveiligingsbeleid.

Specifieke beveiligingsfuncties
Publieke dienstverlening:
- Beveiligingsbeheerder Basis Registratie Personen
- Controller Informatiebeveiliging Basis Registratie Personen
- Beveiligingsfunctionaris waardedocumenten
- Security Officer Suwi (inkijk Publieke Dienstverlening t.b.v. adresonderzoeken)

De Taken, Verantwoordelijkheden en Bevoegdheden van deze rollen, staan nader beschreven in het Informatiebeveiligingsbeleid Publieke Dienstverlening.

Sociale zaken Maastricht Heuvelland
- Security Officer Suwi (Suwinet SZMH)

De Taken, Verantwoordelijkheden en Bevoegdheden van bovenstaande rol, staat nader beschreven in het Informatiebeveiligingsbeleid Publieke Dienstverlening.

Management lijnorganisatie
- Geeft invulling aan het vastgestelde informatiebeveiligingsbeleid en de daaruit voortvloeiende informatiebeveiligingsdoelstellingen door de vertaling in concrete operationele beheersmaatregelen. Zij draagt tevens zorg voor verdere implementatie en handhaving.
- Is eigenaar van de risico's en de te implementeren maatregelen;

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.ibdgemeenten.nl

- Is verantwoordelijk voor de (keten)processen die onder hun verantwoordelijkheid vallen inclusief informatiebeveiliging en draagt zorg voor het actueel houden van het informatie security management systeem (ISMS) voor zijn processen en voor de bevordering en borging van het bewustzijn ten aanzien van informatiebeveiliging bij medewerkers;

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

Overlegstructuur informatieveiligheid

- **Strategisch Informatiebeveiligingsoverleg** (richten)

Het strategisch informatiebeveiligingsoverleg vindt zo vaak plaats als nodig is; deelnemers zijn de portefeuillehouder informatieveiligheid, de directeur bedrijfsvoering/CIO en de CISO, als onderdeel van het reguliere PO IBD. Het overleg richt zich op de strategische richting die de gemeente Maastricht aangaande informatieveiligheid wenst op te gaan.

- **Tactisch Informatiebeveiligingsoverleg** (inrichten)

Vindt 2-wekelijks plaats, deelnemers: CISO, FG. Adviseur Audit & Control en specialist informatiebeveiliging. Het overleg heeft onder meer binnen de gemeente een adviesfunctie richting bestuur en management van de organisatie. Het overleg richt zich op beleid en adviseert gevraagd en ongevraagd over vraagstukken aangaande informatiebeveiliging.
Op ad-hoc basis worden per onderwerp eventueel andere deelnemers uitgenodigd.

- **Operationeel Informatiebeveiligings- en privacyoverleg** (verrichten)

Wekelijks vergadert het C(omputer)E(mergency)R(esponse)T(eam). Aan het overleg nemen deel: CISO. Specialist informatiebeveiliging, Systeem architect, Infrastructuur architect, Infrabeheerder(s) en Licentiebeheerder. Op ad-hoc basis worden per onderwerp eventueel andere deelnemers uitgenodigd.

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

De verantwoording over informatieveiligheid komt tot uitdrukking in de jaarlijkse collegeverklaring Informatiebeveiliging en het 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.

Aldus besloten door het College van Burgemeester en Wethouders van Maastricht d.d. 8 november 2022.

De Secretaris,
G.J.C. Kusters

De Burgemeester,
J.M. Penn-te Strake