Strategisch Informatiebeveiligingsbeleid

Gemeente Maastricht

Colofon

Naam document
Strategisch informatiebeveiligingsbeleid gemeente Maastricht.

Versienummer
1.0

Versie datum
06-09-2019

Vaststelling
Het strategisch informatiebeveiligingsbeleid is vastgesteld door het college van B&W van de gemeente Maastricht op xx.xx.2019.

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

Met dank aan
De informatiebeveiligingsdienst voor gemeenten (IBD) voor het beschikbaar stellen van relevante documentatie die als input heeft gediend voor dit document.

Inhoudsopgave

Strategisch informatiebeveiligingsbeleid

Inleiding

Met dit 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.

Dit document beschrijft het strategische informatiebeveiligingsbeleid van de gemeente Maastricht voor de periode 2020-2023 en vervangt het in 2015 vastgestelde `Informatiebeveiligingsbeleid gemeente Maastricht'. Het voorgaande beleid gebaseerd op de baseline informatiebeveiliging gemeenten gaf een eerste invulling/ handreiking voor het normenkader dat hierin benoemd werd. Dit nieuwe beleid verwijst direct naar de baseline informatiebeveiliging overheid (BIO; als opvolger van de BIG) 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 baseline informatiebeveiliging overheid en de 10 bestuurlijke principes voor informatiebeveiliging.

Baseline Informatiebeveiliging Overheid

Met ingang van 2020 is de baseline informatiebeveiliging overheid (BIO, bijlage 1) het vigerende normenkader voor de overheid en vervangt daarmee de baseline informatiebeveiliging Nederlandse gemeenten (BIG) die tot eind 2019 van kracht blijft. De werkwijze van de BIO is meer gericht op risicomanagement dan de BIG. 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.

10 Bestuurlijke principes voor informatiebeveiliging

De 10 bestuurlijke principes (bijlage 2) 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;

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

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

Het strategisch informatiebeveiligingsbeleid geldt voor alle processen van de gemeente Maastricht en borgt daarmee de veiligheid van de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beleid heeft naast ICT, ook betrekking op:

- Toegangsbeveiliging, fysieke beveiliging en beveiliging van de omgeving;
- In-, door- en uitstroom van medewerkers;
- Leveranciersrelaties;
- Gedragsregels voor bezoekers.

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

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, levert de opdrachtnemer een TPM-verklaring op waarmee assurance door een onafhankelijke derde partij wordt afgegeven over de kwaliteitsaspecten integriteit, beschikbaarheid en vertrouwelijkheid. (Bij voorkeur een ISAE 3402 type 2 verklaring);
- 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, tevens CIO;
- Er een meerjarig informatiebeveiligingsplan is opgesteld gebaseerd op:
    - 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];

[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

- Aandachtspunten ten aanzien van informatiebeveiliging afkomstig van de managers bedrijfsvoering en de teammanagers 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.

De **Directeur bedrijfsvoering/CIO** is samen met het **Managementteam Bedrijfsvoering**:

- 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;
- Gemandateerd bevoegd en verantwoordelijk voor het vaststellen van het meerjarig informatiebeveiligingsplan.

Chief Information Security Officer (CISO, bijlage 3)
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 het meerjarige informatiebeveiligingsplan;
- Het rapporteren over de uitvoering en voortgang van het meerjarig informatiebeveiligingsplan aan de Directeur bedrijfsvoering/CIO en het Managementteam Bedrijfsvoering;
- Het geven van gevraagd en ongevraagd advies aan het bestuur en het management van de organisatie over te nemen maatregelen.

Concernzaken

- Ondersteunt de gemeentelijke organisatie door de inzet van een CISO;
- Toetst op verzoek door de business opgestelde en geïmplementeerde informatiebeveiligings-maatregelen op opzet, bestaan en effectieve werking, waarbij de focus ligt bij het cluster control;
- Draagt bij aan de vertaling en invulling van informatiebeveiliging binnen het organisatiebrede (informatie)beleid en de planning daarvan, waarbij de focus ligt bij het cluster informatisering & automatisering (I&A).

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. Binnen de lijnorganisatie is qua verantwoordelijkheid een verdere opsplitsing te maken:

- **Manager organisatieonderdeel/manager bedrijfsvoering**
  Is eigenaar van de risico's en de te implementeren maatregelen;

- **Teammanager**
  Is verantwoordelijk voor de (keten)processen die onder zijn 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 zijn medewerkers;
- **Medewerkers** zijn verantwoordelijk voor het zorgvuldig omgaan met persoonsgegevens en andere (vertrouwelijke) informatie waar zij uit hoofde van hun functie toegang toe hebben.

Shared Service Center
Het Shared Service Center ondersteunt de gemeentelijke organisatie door de inzet van informatie-beveiligingsspecialisten voor:

- Uitvoering geven aan het informatiebeveiligingsbeleid en -plan;
- Uitvoering geven aan en mede ontwikkelen van beleid gericht op informatiebeveiliging;
- Identificering en analysering van beveiligingsrisico's en het formuleren van verbetervoorstellen;
- Ondersteunen van het lijnmanagement bij informatiebeveiligingsvraagstukken.

Overlegstructuur informatieveiligheid

- **Strategisch Informatiebeveiligingsoverleg** (richten)

Het strategisch informatiebeveiligingsoverleg vindt zo vaak plaats als nodig is; deelnemers zijn de portefeuillehouder informatieveiligheid, de gemeentesecretaris, 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)

Het tactisch informatiebeveilingsoverleg vindt zo vaak als nodig is plaats, maar minimaal 3 keer per jaar, als onderdeel van de reguliere overlegstructuur van het MTBV en is besluitvormend van aard.

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

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

Verantwoording

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