MONTFOORT

# GEMEENTEBLAD

Officiële uitgave van de gemeente Montfoort

Nr. 76211

21 februari

2024

## Strategisch Informatiebeveiligingsbeleid 2023 en verder

**1 Inleiding**
Deze beleidsnota[1] beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2023 en verder en vervangt het in 2021 vastgestelde 'Strategisch Informatiebeveiligingsbeleid 2021-2023'. Deze nota is richtinggevend en wordt aangevuld met specifieke beleidsdocumenten[2] voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau. Met dit beleid zet de gemeente Montfoort een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO)[3]. De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG[4].

**Leeswijzer**
In het eerste deel wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke aanvullingen. In het jaarlijks op te stellen Uitvoeringsplan Informatiebeveiligingsbeleid (vastgesteld door het Directie Team (DT)) worden de tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt door de CISO gedaan op basis van input van het DT, de Concernmanagers, Teamcoördinatoren, de CISO, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA. Hier staan ook de acties in vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid wordt geëist. Het tweede deel van dit document beschrijft hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

**Wat is informatiebeveiliging?**
Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.
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 bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

**Plaats van het strategisch beleid**
Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het Uitvoeringsplan.

**Ambitie en visie**
Informatieveiligheid is een van de voorwaarden om de ambities en doelen uit het Uitvoeringsprogramma college 2022-2026 gemeente Montfoort[5] te realiseren. Een veilige informatievoorziening en informatiestructuur maakt het mogelijk om risico's met betrekking tot informatiebeveiligingsincidenten te reduceren tot een, door het DT vastgesteld, acceptabel niveau.

**Scope informatiebeveiliging**
De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, 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 gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt ook aanvullende beveiligingseisen uit wetgeving af zoals voor de Basis Registratie Personen. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd. Bewust is in dit strategisch beleid geen limitatief overzicht van alle onderliggende documenten opgenomen. Andersom wordt in deze documenten de link naar het strategisch beleid wel gelegd.

**2 Strategisch beleid**

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2023 en verder'. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen Uitvoeringsplan Informatiebeveiligingsbeleid.

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn hieronder uitgewerkt.

**De BIO**
De BIO (Baseline Informatiebeveiliging Overheid) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de Teamcoördinatoren meer dan nu gebeurt moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

**10 principes voor informatiebeveiliging**
De onderstaande principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO[6] en gaan over de waarden die de bestuurder zichzelf oplegt.

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.

Deze principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente.

**Dreigingsbeeld**
Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

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

**Standaarden informatiebeveiliging**
De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017. Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[7] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van deze beide NEN-normen.
De Baseline Informatiebeveiliging Overheid omvat verschillende niveaus van beveiligen. Ook worden er praktische operationele handreikingen uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan. Het Uitvoeringsplan zal de structuur van de BIO volgen.
Binnen de gemeente wordt naast ICT ook Operationele Technologie ingezet (bv techniek rond verkeerslichteninstallatie of riolen en gemalen). Ook deze systemen vallen binnen het beveiligingsbeleid van de gemeente en dit beleid betreft dus ook beleidsteams die zich met deze procesautomatisering bezighouden.

**Uitgangspunten**
Het bestuur en de directie spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. De directie maakt een inschatting van het belang dat de verschillende delen van de infor-

matievoorziening voor de gemeente hebben, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Op basis hiervan zet de directie dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan. De directie geeft richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente.

Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

**Strategische doelen informatiebeveiligingsbeleid**
* 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.

**Belangrijkste uitgangspunten van het beleid:**
* Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van B en W is eindverantwoordelijke voor de informatiebeveiliging.
* De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de Gemeente Montfoort hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
* Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het Uitvoeringsplan het fundament onder een betrouwbare informatievoorziening. In het Uitvoeringsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
* Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het systeem van informatiebeveiliging.
* De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
* Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
* Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

**Praktisch invulling aan de uitgangspunten:**
* Het college van B en W stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
* Het DT stelt jaarlijks het bijbehorende Uitvoeringsplan bij het Informatiebeveiligingsbeleid vast.
* Het DT is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
* Het DT is verantwoordelijk voor het vragen om informatie bij de Teamcoördinatoren en ziet erop toe dat adequate maatregelen genomen worden voor de bescherming van de informatie, informatiesystemen en procesautomatiseringssystemen die onder hun verantwoordelijkheid valt.
* De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het DT..
* Het DT stuurt de Teamcoördinatoren aan voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
* De CISO en de Teamcoördinatoren zijn verantwoordelijk voor het oefenen met informatiebeveiligingsincidenten..

* Hoewel de kernregistraties (zoals BRP, PUN, SUWI, BAG, BGT, BRO) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
* Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
* Medewerkers moeten verantwoord omgaan met persoonsgegevens en andere informatie.
* De directie moet erop toezien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kan vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
* De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teamcoördinatoren toetsen zelf hun processen op informatieveiligheid op basis van de BIO.
* Informatiebeveiliging maakt deel uit van de beoordelingssystematiek en wordt besproken tussen het DT en de Teamcoördinator én door de Teamcoördinator en zijn/haar medewerkers.

**Belangrijke randvoorwaarden zijn:**
De informatiebeveiliging maakt deel uit van afspraken met ketenpartners. Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden. Jaarlijks wordt een Uitvoeringsplan opgesteld door de CISO, gebaseerd op:
* de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
* het dreigingsbeeld gemeenten van de IBD;
* De door het DT, de concernmanagers en de Teamcoördinatoren ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse.

**3 Organisatie, taken & verantwoordelijkheden**
In dit deel wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence. In dit model zijn de Teamcoördinatoren verantwoordelijk voor de eigen processen. De CISO (2e lijn) ondersteunt, adviseert en coördineert de Teamcoördinatoren. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

**Aansturing: Directieteam**
Het DT zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een Teamcoördinator. Het DT zorgt dat de Teamcoördinatoren zich verantwoorden over de beveiliging van de informatie waar zij verantwoordelijk voor zijn. De directie zorgt dat de portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de informatiebeveiliging als onderdeel van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.
Het DT stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het DT draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente. Het DT autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de gemeente Montfoort gezien als een integraal onderdeel van risicomanagement.

**Uitvoering: Teamcoördinatoren**
Informatiebeveiliging valt onder de verantwoordelijkheden van alle Teamcoördinatoren. Om deze verantwoordelijkheid waar te maken worden zij ondersteund door de CISO. Deze verantwoordelijkheid kan de Teamcoördinator niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teamcoördinatoren rapporteren aan het DT over de tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de teams over de inhoudelijke aanpak vindt plaats door het onderwerp Informatiebeveiliging regelmatig te bespreken in het Teamcoördinatorenoverleg.

Taken van de Teamcoördinatoren in het kader van informatiebeveiliging zijn:
* Het leveren van input voor wijzigingen op maatregelen en procedures.
* Het voldoen aan wetgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wetgeving bedacht is.
* Het binnen het eigen team uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures.
* Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
* Bespreking van beveiligingsincidenten en de consequenties die deze moeten hebben voor beleid en maatregelen.

**Controle en verantwoording**
Dit Strategisch Beleid is een verantwoordelijkheid van het bestuur van de gemeente Montfoort. De bestuurders en directeuren van de gemeente Montfoort zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

Het DT is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. Het DT rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel-) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

**ENSIA**
De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat jaarlijks een ENSIA-coördinator wordt aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke Teamcoördinator. De Teamcoördinatoren leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.

Met deze verantwoording worden het bestuur van de gemeente Montfoort en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Montfoort informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

**Bijlage DigiD aansluiting (norm B.01)**
In aanvulling op dit informatiebeveiligingsbeleid zijn voor de DigiD aansluiting de volgende aanvullende maatregelen en verantwoordelijkheden van toepassing:

Normen
We conformeren ons aan de laatste door Logius gepubliceerde Norm ICT-beveiligingsassessments DigiD versie 3.0.
Jaarlijks wordt dit normenstelsel in het kader van ENSIA door een externe auditor en CISO getoetst. Over deze toetsing vindt horizontaal (van college aan de raad) en verticaal (naar Logius) verantwoording plaats.

Eigenaarschap
Geheel in lijn met de BIO is het eigenaarschap van de DigiD-webapplicaties (de webapplicaties die de DigiD-functionaliteit als module aanroepen) belegd in de lijnorganisatie en is de betreffende Marc van der Veer (Gemeentesecretaris) eindverantwoordelijk voor het goed functioneren van de applicatie en de te treffen maatregelen.

Functioneel beheer
Per DigiD-aansluiting is door de genoemde leidinggevende een functioneel beheerder bij team Processen en Gegevens aangewezen die de verantwoordelijkheid heeft de door Logius opgestelde beveiligingsnormen te implementeren, controleren (middels een jaarlijkse TPM-verklaring) en bewijslast ervan op te bouwen in een auditdossier.
Het auditdossier wordt jaarlijks aan onze externe auditor beschikbaar gesteld en bevat tenminste de contracten en servicerapportages van onze SaaS-leverancier(s) (norm B.05), de incidentprocedure en een overzicht van de incidenten (U/WA.02), de dataclassificatie (U/WA.05), bewijs dat de webapplicatie gehardend is (U/NW.06, tav DNSSEC) en de beoordeelde releases (C.08).
Tweemaal per jaar (geagendeerd) wordt er door functioneel beheer beoordeeld of alle autorisaties compleet en actueel zijn; hierover wordt verslag (autorisatiematrix) gedaan richting verantwoordelijk leidinggevende.

Technisch
Wij maken – voor wat betreft DigiD-aansluitingen - uitsluitend gebruik van cloudapplicaties die door SaaS-leveranciers worden geleverd. Daarom wordt een groot deel van de door Logius afgekondigde normen ingevuld door de SaaS-leverancier die hiervan middels een jaarlijkse – door een onafhankelijk auditor opgestelde - TPM-verklaring verantwoording over aflegt.

Gebruikte afkortingen

**NEN** Afkorting van NEderlandse Norm -> Met NEN worden door de Stichting Koninklijk Nederlands Normalisatie Instituut afspraken vastgelegd in normen en richtlijnen.
**ISO** International Standardization Organization;
**BIO** Baseline Informatiebeveiliging Overheid; De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen).
**CISO** Chief Information Security Officer. De CISO verantwoordelijk is voor het implementeren van informatiebeveiligingsbeleid én het toezicht daarop.
**ENSIA** Gemeenten verantwoorden zich over informatiebeveiliging en kwaliteit middels ENSIA. De afkorting staat voor Eenduidige Normatiek Single Information Audit.
**IBB** De IBD is het Computer Emergency Response Team, of Computer Security Incident Response Team voor alle Nederlandse gemeenten, en onderdeel van de Vereniging van Nederlandse Gemeenten. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy.
**SUWI** Wet structuur uitvoeringsorganisatie werk en inkomen

BRP, PUN, BAG, BGT en de BRO zijn de afkortingen voor respectievelijk Basis Registratie Personen, Paspoort Uitvoeringsregeling Nederland, Basisregistratie Adressen en Gebouwen, Basisregistratie Grootschalige Topografie en de Basisregistratie Ondergrond.

[1] Dit document is gebaseerd op het voorbeeld Informatiebeveiligingsbeleid wat door de IBD beschikbaar is gesteld.
https://www.informatiebeveiligingsdienst.nl/product/voorbeeld-strategisch-gemeentelijk-informatiebeveiligingsbeleid/
[2] Onder andere het Privacy beleid gemeente Montfoort en het Uitvoeringsplan Informatiebeveiligingsbeleid.
[3] https://www.bio-overheid.nl/
[4] De 10 principes voor informatiebeveiliging: https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf
[5] Uitvoeringsprogramma college 2022-2026 gemeente Montfoort
[6] Deze principes zijn gelijk met de BIO van kracht geworden, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG)
***[7]*** De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van de VNG en de IBD, maar ook waterschappen, provincies en het rijk.