STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 5405
23 februari 2024

Regeling van de Minister van Justitie en Veiligheid van 13 februari 2024, kenmerk 4644372, inzake het strategisch kader informatiebeveiliging voor de meldkamervoorzieningen die door de hoofdgebruikers worden gebruikt bij de uitvoering van hun meldkamerfunctie en worden beheerd door de beheerder (Strategisch kader informatiebeveiliging meldkamervoorzieningen)

De Minister van Justitie en Veiligheid, in overeenstemming met de Minister van Defensie,

Gelet op artikel 23, eerste en tweede lid, van de Politiewet 2012;

Besluit:

Artikel 1 Begrippen

In dit strategisch kader wordt verstaan onder:
a) *meldkamervoorzieningen:* alle gemeenschappelijke voorzieningen, waaronder ICT voorzieningen, die gebruikt worden door een of meer hoofdgebruikers bij de uitvoering van hun meldkamerfunctie én die door de beheerder worden beheerd.
b) *beheer:* facilitaire dienstverlening, huisvesting, inrichting, onderhoud en ontwikkeling van gemeenschappelijke ICT-voorzieningen ten behoeve van de meldkamers en het ICT-beheer ten behoeve van de meldkamerfuncties;
c) *beheerder meldkamervoorzieningen:* korpschef van de politie, bedoeld in artikel 1, aanhef en onder c, van de Politiewet 2012;
d) *Landelijke Meldkamer Samenwerking:* het onderdeel van de politie waar het beheer van de meldkamers, bedoeld in artikel 25a van de Politiewet 2012, is ondergebracht;
e) *partijen:* de Minister voor Medische Zorg en de Regionale Ambulancevoorzieningen voor zover het de ambulancezorg betreft, de besturen van de veiligheidsregio's voor zover het de brandweertaak, de rampenbestrijding, de crisisbeheersing en de geneeskundige hulpverlening hierbij betreft, de Minister van Defensie voor zover het de Koninklijke marechaussee betreft, de Minister van Justitie en Veiligheid en de politie;
f) *hoofdgebruikers:* de hulpdiensten politie, ambulance, brandweer en de Koninklijke Marechaussee. Defensie is in plaats van de Koninklijke Marechaussee een hoofdgebruiker voor zover het de C2000 communicatievoorziening betreft.
g) *medegebruiker:* een andere gebruiker dan de hoofdgebruikers die uit oogpunt van openbare orde, veiligheid of hulpverlening in contact moeten kunnen treden met een of meer hoofdgebruikers ofwel anderszins voor een hoofdgebruiker aantoonbaar operationeel belang heeft om gebruik te maken van meldkamervoorzieningen.
h) *multidisciplinaire sturingslijn:* de sturingslijn die wordt gevormd door het Bestuurlijk Meldkamer Beraad, bedoeld in artikel 3, eerste lid, van de Regeling hoofdlijnen beleid en beheer meldkamers, en het Strategisch Meldkamer Beraad, bedoeld in artikel 4, eerste lid, van die regeling;
i) *informatiebeveiligingsbeleid meldkamervoorzieningen:* het geheel aan uitgangspunten, randvoorwaarden en regels ten aanzien van het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede ten aanzien van het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen, als het neerleggen van de taken en verantwoordelijkheden bij de verschillende organisaties horende bij het beheer en gebruik van de meldkamervoorzieningen;
j) *BIO:* Baseline Informatiebeveiliging Overheid, bedoeld in de Circulaire toepassen Baseline Informatiebeveiliging Overheid in het digitale verkeer met het Rijk;
k) *ICV:* in-controlverklaring, een beschrijving van de kwaliteit van de bedrijfsvoering van de betreffende organisatie met betrekking tot de verplichtingen die voortvloeien uit deze regeling en het informatiebeveiligingsbeleidsbeleid meldkamervoorzieningen.

Artikel 2 Algemeen kader

1. De informatiebeveiliging van de meldkamervoorzieningen wordt ingericht volgens ten minste de BIO.

2. Er dient door de hoofdgebruikers, in afstemming met de beheerder, een informatiebeveiligingsbe-

leid meldkamervoorzieningen te worden opgesteld. Het informatiebeveiligingsbeleid bevat in ieder geval:
a. de nadere invulling van taken, verantwoordelijkheden en bevoegdheden van de hoofdgebruikers en de beheerder rondom het informatiebeveiligingsbeleid van de meldkamervoorzieningen;
b. de gemeenschappelijke eisen, in het bijzonder de maatregelen die volgen uit het basisbeveiligingsniveau; en
c. de gemeenschappelijke normen met betrekking tot het informatiebeveiligingsbeleid van de meldkamervoorzieningen.

3. De beheerder en de hoofdgebruikers stellen een implementatieplan op. In dit implementatieplan is inzichtelijk op welke wijze dit kader en het informatiebeveiligingsbeleid, of een wijziging van het strategisch kader of het informatiebeveiligingsbeleid, binnen de eigen organisatie wordt geïmplementeerd en toegepast.

4. De beheerder en de hoofdgebruikers rapporteren periodiek over de voortgang van de uitvoering van de implementatieplannen aan de multidisciplinaire sturingslijn via de PDCA-cyclus van het beleids- en bestedingsplan meldkamers.

Artikel 3 Bestuurlijk Meldkamer Beraad en Strategisch Meldkamer Beraad

1. Wijziging van het informatiebeveiligingsbeleid van de meldkamervoorzieningen vindt plaats na overleg met het Strategisch Meldkamer Beraad, bedoeld in artikel 4, eerste lid, van de Regeling hoofdlijnen beleid en beheer meldkamers, en wordt vastgesteld door het Bestuurlijk Meldkamer Beraad, bedoeld in artikel 3, eerste lid, van die regeling.

2. Er is een beleids- en bestedingsplan, bedoeld in artikel 6, eerste en tweede lid, van de Regeling hoofdlijnen beleid en beheer meldkamers. Het informatiebeveiligingsbeleid van de meldkamervoorzieningen is onderdeel van het beleids- en bestedingsplan.

3. Het Strategisch Meldkamer Beraad monitort het beleids- en bestedingsplan meldkamers en het hierin opgenomen informatiebeveiligingsbeleid van de meldkamervoorzieningen en adviseert het Bestuurlijk Meldkamer Beraad hierover.

4. De partijen dragen jaarlijks hun wensen met betrekking tot de informatiebeveiliging van de meldkamervoorzieningen voor het beleids- en bestedingsplan aan.

5. In het Strategisch Meldkamer Beraad worden jaarlijks de ICV's van de beheerder en hoofdgebruikers besproken. In het Bestuurlijk Meldkamer Beraad vindt hierover, horende het advies van het Strategisch Meldkamer Beraad, besluitvorming plaats.

6. Het Bestuurlijk Meldkamer Beraad kan, horende het advies van het Strategisch Meldkamer Beraad, onderzoek laten uitvoeren naar de werking van het informatiebeveiligingsbeleid meldkamervoorzieningen en aanwijzingen geven voor verbetering.

7. Voor het realiseren van de taken, zoals genoemd in dit artikel, kan het Strategisch Meldkamer Beraad een hulpstructuur instellen.

Artikel 4 Beheerder meldkamervoorzieningen

1. De beheerder is verantwoordelijk voor het implementeren en naleven van het informatiebeveiligingsbeleid meldkamervoorzieningen door de eigen organisatie.

2. De beheerder richt een risicomanagementproces in voor de gemeenschappelijke meldkamervoorzieningen, conform de normen van de BIO, en in het bijzonder het bepaalde basis beveiligingsniveau. De beheerder betrekt en consulteert de hoofdgebruikers bij dit risicomanagementproces en de bijbehorende risicoanalyses.

3. De beheerder bereidt de besluitvorming in de multidisciplinaire sturingslijn voor ten aanzien van de vaststelling en wijziging van het informatiebeveiligingsbeleid meldkamervoorzieningen. Dit doet de beheerder in samenwerking met de hoofdgebruikers. De beheerder neemt in elk geval het initiatief het informatiebeveiligingsbeleid bij te stellen of te wijzigen:
a. als de jaaraanschrijving daartoe aanleiding geeft; en
b. als de door hem op te stellen risicoanalyse over zijn beheerstaken daartoe aanleiding geeft.

4. De beheerder monitort de naleving van het informatiebeveiligingsbeleid meldkamervoorzieningen door de eigen organisatie.

5. De beheerder stelt jaarlijks een ICV op ten aanzien van het beheer van de meldkamervoorzieningen.

Artikel 5 Hoofdgebruikers en medegebruikers meldkamervoorziening

1. Elke hoofdgebruiker is zelf verantwoordelijk voor het implementeren en naleven van het voor zijn organisatie van toepassing zijnde informatiebeveiligingsbeleid meldkamervoorzieningen binnen de eigen organisatie.

2. Elke hoofdgebruiker richt een risicomanagementproces in voor de door hem gebruikte meldkamervoorzieningen, conform de normen van de BIO, en in het bijzonder het bepaalde basis beveiligingsniveau.

3. De hoofdgebruiker monitort de naleving van het informatiebeveiligingsbeleid meldkamervoorzieningen door de eigen organisatie.

4. Elke hoofdgebruiker is zelf verantwoordelijk voor het implementeren en naleven van het informatiebeveiligingsbeleid meldkamervoorzieningen door medegebruikers die onder zijn verantwoordelijkheid vallen.

5. Elke hoofdgebruiker is verplicht jaarlijks een ICV af te geven voor bespreking in het Strategisch Meldkamer Beraad. In de ICV van de hoofdgebruiker worden ook de medegebruikers die onder de verantwoordelijkheid van de hoofdgebruiker vallen meegenomen.

Artikel 6 Evaluatie

De Minister van Justitie en Veiligheid zal minstens eens in de vijf jaar de doeltreffendheid en de effecten van het strategisch kader evalueren door middel van audits.

Artikel 7 Inwerkingtreding

Deze regeling treedt in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst.

Artikel 8 Citeertitel

Deze regeling wordt aangehaald als: Strategisch kader informatiebeveiliging meldkamervoorzieningen.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

TOELICHTING

Algemeen

De informatiebeveiliging van de meldkamervoorzieningen is een belangrijk onderwerp waar continu aandacht voor moet zijn en blijven. Als de informatiebeveiliging van de meldkamervoorzieningen niet op orde is, kan dat leiden tot verstoringen in het systeem of het verlies van data. Verstoringen op meldkamervoorzieningen kunnen invloed hebben op het contact tussen burgers en hulpverleners en de meldkamer en hulpverleners onderling wanneer elke seconde telt. Hulpverlening, crisisbeheersing en opsporing lopen dan gevaar.

Om het informatiebeveiligingsbeleid van de gemeenschappelijke meldkamervoorzieningen verder te brengen is een strategisch kader noodzakelijk waarin de verantwoordelijkheden, taken en rollen van de verschillende betrokken organisaties zijn beschreven. Aan de hand hiervan kan het informatiebeveiligingsbeleid steeds nader worden uitgewerkt en geïmplementeerd. Het Strategisch kader informatiebeveiliging meldkamervoorzieningen (hierna: strategisch kader) omarmt de BIO Baseline. Dit betekent dat het informatiebeveiligingsbeleid een continu proces wordt, een vast onderdeel van de werkzaamheden en organisatie van de betrokken organisaties. De beveiliging is namelijk nooit helemaal af. Nieuwe maatschappelijke ontwikkelingen of technologieën kunnen nieuwe dreigingen meebrengen voor de gemeenschappelijke meldkamervoorzieningen. De continue aandacht is dan ook onderdeel van dit strategisch kader.

Voor het goed op orde brengen en houden van de informatiebeveiliging van de meldkamervoorzieningen is het van belang dat het onderwerp informatiebeveiliging bij alle organisaties de noodzakelijke prioriteit krijgt. Iedere organisatie, zowel de hoofdgebruikers, medegebruikers, beheerder, maar ook de Minister van Justitie en Veiligheid als stelselverantwoordelijke, heeft hierin een eigen, maar ook een gezamenlijke verantwoordelijkheid. Iedere organisatie heeft de ander nodig bij het behalen van het gezamenlijke doel – het continu verbeteren, naleven en monitoren van de informatiebeveiliging van de meldkamervoorzieningen.

Stelselverantwoordelijkheid

De Minister van Justitie en Veiligheid is stelselverantwoordelijk voor de inrichting en werking van het meldkamerdomein. De Minister heeft daarbij de taak om de continuïteit van de meldkamers zoveel mogelijk te borgen en ervoor te zorgen dat het meldkamerstelsel robuust en bij de tijd is, wendbaar is en blijft innoveren. Daarnaast faciliteert de Minister de organisaties binnen het meldkamerstelsel om hun taken uit te voeren en maakt de Minister de rollen, taken en verantwoordelijkheden voor iedereen helder.

Op grond van artikel 23 van de Politiewet 2012 kunnen bij ministeriële regeling regels worden gesteld over de informatie- en communicatievoorzieningen van de politie en het gebruik daarvan door de politie en andere organisaties die een taak hebben op het terrein van justitie, openbare orde, veiligheid of hulpverlening, en waarmee de politie ter uitvoering van de politietaak informatie- en communicatievoorzieningen deelt. Daarnaast kunnen nadere regels worden gesteld over de informatiebeveiliging van informatie- en communicatievoorzieningen van de politie.

In artikel 2, tweede lid, aanhef en onder b, van de Regeling hoofdlijnen beleid en beheer meldkamers[1] staat dat de informatiebeveiliging van de meldkamers en meldkamerfuncties voldoet aan de wettelijke kaders en aan de van toepassing zijnde normen van de partijen. In dit strategisch kader worden door de Minister van Justitie en Veiligheid, tevens stelstelverantwoordelijke voor het meldkamerdomein, voorschriften gesteld omtrent de informatieveiligheid van de meldkamervoorzieningen en de taken en verantwoordelijkheden van de betrokken organisaties bij de betreffende voorzieningen. Het strategisch kader beantwoordt de zogenoemde 'wat'-vraag: *Wat is er nodig om de informatieveiligheid van de meldkamervoorzieningen te realiseren*.

Reikwijdte

Het strategisch kader is van toepassing op het gebruik en het beheer van de meldkamervoorzieningen. Het betreft hier alle voorzieningen die op de meldkamers gebruikt worden én die door de Landelijke Meldkamer Samenwerking (hierna: LMS) worden beheerd. Het maakt niet uit voor welke processen de voorzieningen worden gebruikt. Als een meldkamervoorziening door één of meerdere disciplines

[1] Regeling hoofdlijnen beleid en beheer meldkamers: wetten.nl - Regeling - Regeling hoofdlijnen beleid en beheer meldkamers - BWBR0043762 (overheid.nl)

wordt gebruikt én deze meldkamervoorziening in beheer is bij de LMS, is het strategisch kader en het bijbehorend informatiebeveiligingsbeleid meldkamers van toepassing.

Indien een meldkamervoorziening buiten de meldkamer wordt gebruikt, is het strategisch kader ook buiten de meldkamer van toepassing. Te denken valt hierbij aan mobiel gebruik van voorzieningen en communicatiemiddelen, zoals C2000. C2000-randapparatuur wordt door de disciplines op straat gebruikt. Het informatiebeveiligingsbeleid meldkamervoorzieningen stelt eisen aan het gebruik en beheer van de randapparatuur omdat deze gebruik maken van het C2000-communicatienetwerk. Dit geldt verder voor andere apparatuur (zoals mobiele telefoons en laptops) waarmee gebruik wordt gemaakt van de meldkamervoorzieningen en voor (delen van) processen die buiten de vastgestelde meldkamerlocaties plaatsvinden en waarvoor meldkamervoorzieningen worden gebruikt.

Thans vallen de volgende meldkamervoorzieningen onder het strategisch kader:
- Voorziening Spoedvraag;
- Voorziening Spoedrespons;
- Voorziening Gemeenschappelijk Meldkamer Systeem;
- Voorziening Ondersteunende informatiesystemen;
- Voorziening IV/ICT infrastructuur; en
- Voorziening Huisvesting en facilitaire services.

Aansluiting Regeling hoofdlijnen beleid en beheer meldkamers

Het strategisch kader en bijbehorend informatiebeveiligingsbeleid meldkamervoorzieningen wordt beheerd door de Landelijke Meldkamer Samenwerking (LMS). De LMS, ondergebracht bij de politie, opereert binnen de governancestructuur ingericht voor de gezamenlijke multidisciplinaire sturing op het beheer van de meldkamers en de gezamenlijke meldkamervoorzieningen.

In lijn met de Regeling hoofdlijnen beleid en beheer meldkamers zal de verantwoording over de informatieveiligheid van de meldkamervoorzieningen plaatsvinden via de sturingslijn van de multigovernance voor het beheer van de meldkamers. Deze verantwoording is ook voorgeschreven in de BIO Baseline.

Artikelsgewijze toelichting

Artikel 2

In dit artikel wordt het algemeen kader beschreven waaraan de informatiebeveiliging van de meldkamervoorzieningen dient te voldoen. In het **eerste lid** is neergelegd dat de informatiebeveiliging van de meldkamervoorzieningen dient te worden ingericht volgens tenminste de Baseline Informatiebeveiliging Overheid (BIO). De BIO beschrijft de invulling van de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 voor de overheid. Daarnaast kunnen de gebruikers specifieke normen hanteren inzake informatiebeveiliging horende bij hun taak. Denk hierbij aan de NEN 7510, voor de zorg. In het informatiebeveiligingsbeleid en het daarbij behorende BIO addendum wordt met de verschillende normenkaders rekening gehouden om de verschillende maatregelen zo werkbaar mogelijk te maken.

De BIO dient in alle lagen en niveaus van de betrokken organisaties te worden geïmplementeerd. Verplichtingen die reeds in andere wet- en regelgeving zijn neergelegd rondom informatiebeveiliging en de omgang met vertrouwelijke (persoons)gegevens – zoals in de Algemene verordening gegevensbescherming, de Wet Beveiliging Netwerk- en Informatiesystemen, de Wet politiegegevens en de Wet op de Geneeskundige Behandelingsovereenkomst – zijn niet apart in dit strategisch kader benoemd. De van toepassing zijnde verplichtingen uit deze wet- en regelgeving dienen additioneel te worden geïmplementeerd.

Een belangrijk onderdeel van de BIO betreft het risicomanagementproces, de PDCA-cyclus (Plan-Do-Check-Act). Door een risicomanagementproces in te richten kunnen de hoofdgebruikers en beheerder op een goede manier risico's identificeren, beoordelen, sturen en beheersen. Het helpt om in control te komen, de risico's inzichtelijk te hebben en daar eventueel maatregelen tegen te nemen, en om continu te verbeteren door cyclisch te werk te gaan.

In het **tweede lid** is neergelegd dat er een informatiebeveiligingsbeleid meldkamervoorzieningen door de hoofdgebruikers, in afstemming met de beheerder, dient te worden opgesteld. Hiervoor is een werkgroep informatiebeveiligingsbeleid opgericht, waaraan de hoofdgebruikers, de beheerder en het Ministerie van Justitie en Veiligheid deelnemen. De werkgroep rapporteert aan het Strategisch Meldkamer Beraad en legt daar het informatiebeveiligingsbeleid ter besluitvorming voor.

In het strategisch kader is opgenomen welke onderwerpen in ieder geval in het informatiebeveiligingsbeleid dienen te worden behandeld. Zo dienen in het informatiebeveiligingsbeleid de rollen, taken en verantwoordelijkheden, op basis van dit strategisch kader, verder te worden uitgewerkt. Daarnaast dienen de gemeenschappelijke betrouwbaarheidseisen te worden beschreven en regelmatig te worden herijkt. De betrouwbaarheidseisen richten zich op de beschikbaarheid, integriteit en vertrouwelijkheid van de gemeenschappelijke meldkamervoorzieningen. In het bijzonder heeft de beschikbaarheid van de meldkamervoorzieningen, denk bijvoorbeeld aan C2000 en het Gemeenschappelijk Meldkamer Systeem, hier de aandacht.

Onder het informatiebeveiligingsbeleid meldkamervoorzieningen zal een bioaddendum liggen. In dit addendum zullen per onderwerp / maatregel beleidsregels worden neergelegd. Dit betreffen onderwerpen (niet limitatief) als toegangsbeveiliging, cryptografie, beheer apparatuur, gebruiks- en beheerprocedures, logging en monitoring, informatiedeling en gegevensrubricering. Onderwerpen die nu ook deels in de beleidsregel informatiebeveiliging C2000 zijn vervat. Met de komst van dit strategisch kader en het informatiebeveiligingsbeleid meldkamervoorzieningen is de aparte beleidsregel informatiebeveiliging C2000 niet langer noodzakelijk. De beleidsregel zal worden ingetrokken. Gelet op het vitale proces van de C2000 communicatievoorziening, zal in het informatiebeveiligingsbeleid meldkamervoorzieningen specifieke aandacht zijn voor de Voorziening Spoedrespons (C2000).

In het **derde lid** is geregeld dat de beheerder en hoofdgebruikers een implementatieplan opstellen. Informatiebeveiliging is belangrijk en noodzakelijk en moet in alle lagen en niveaus van het meldkamerstelsel worden geïmplementeerd. Een implementatieplan is daarbij noodzakelijk. De beheerder en de hoofdgebruikers rapporteren periodiek over de voortgang van de uitvoering van de implementatieplannen aan de multidisciplinaire sturingslijn – het Strategisch Meldkamer Beraad en Bestuurlijk Meldkamer Beraad, conform de Regeling hoofdlijnen beleid en beheer meldkamers – via de cyclus van het beleids- en bestedingsplan meldkamers (**lid 4**). Zie hiervoor artikel 3 van het strategisch kader.

Artikel 3

In de artikelen 3 tot en met 5 worden de verantwoordelijkheden en taken van het Bestuurlijk Meldkamer Beraad en Strategisch Meldkamer Beraad beschreven, van de beheerder en van de hoofdgebruikers en medegebruikers. Deze taken en verantwoordelijkheden zijn in lijn met de BIO Baseline. De taken en verantwoordelijkheden zijn op stelselniveau beschreven. Uit artikel 2 volgt dat tenminste de BIO dient te worden geïmplementeerd in alle lagen en niveaus van de betrokken organisaties. In het informatiebeveiligingsbeleid meldkamervoorzieningen dient nader gespecificeerd te worden wat de verschillende verantwoordelijkheden, taken en bevoegdheden zijn op de verschillende niveaus en waar deze liggen.

Met de inwerkingtreding van dit strategisch kader wordt duidelijker neergezet wat de taken en verantwoordelijkheden van de verschillende partijen zijn rondom de informatiebeveiliging van de gemeenschappelijke meldkamervoorzieningen. Dit is geen overbodige luxe in het multidisciplinaire landschap waar het meldkamerstelstel zich in begeeft.

In artikel 3 worden de taken van het Bestuurlijk Meldkamer Beraad en het Strategisch Meldkamer Beraad beschreven, binnen de kaders zoals ook omschreven in de Regeling hoofdlijnen beleid en beheer meldkamers (**lid 1**). Zoals ook in artikel 6 van de Regeling hoofdlijnen beleid en beheer meldkamers staat, wordt hier herhaald dat er een beleids- en bestedingsplan is en dat het informatiebeveiligingsbeleid van de meldkamersystemen hier onderdeel van uitmaakt (**lid 2**). Alle betrokken partijen hebben via de beleids- en beheercyclus invloed op de totstandkoming van het beleids- en bestedingsplan. Het beleids- en bestedingsplan voor de meldkamer wordt binnen de aangegeven beleidsdoelen en beleidskaders van de regeling jaarlijks vastgesteld. Eén van de beleidskaders betreft “de informatieveiligheid van de meldkamers en meldkamerfuncties voldoet aan de wettelijke kaders en aan de van toepassing zijnde normen van de partijen” (artikel 2, tweede lid, aanhef en onder b, van de Regeling hoofdlijnen beleid en beheer meldkamers). Daar valt dit strategisch kader en het bijbehorende informatiebeveiligingsbeleid onder.

De verantwoording over de informatiebeveiliging van de meldkamervoorzieningen vindt plaats via de beleids- en beheercyclus voor het beheer van de meldkamers. Het Strategisch meldkamerberaad draagt zorg (niet limitatief) voor de landelijke strategische sturing op het beleid en beheer van de meldkamers, beslist binnen de kaders van het beleids- en bestedingsplan over de uitvoering van beleid en beheer en bewaakt de uitvoering van het beleids- en bestedingsplan. Het Bestuurlijk Meldkamerberaad monitort de werking van het beleid en beheer van de meldkamers en beslist over voorstellen van het Strategisch Meldkamer Beraad die binnen het vastgestelde beleids- en bestedingsplan bestuurlijke borging behoeven (**lid 3**).

Hoewel uitgebreid beschreven in artikel 6 van de Regeling hoofdlijnen beleid en beheer meldkamers

wordt hier nog specifiek benoemd dat partijen jaarlijks hun wensen met betrekking tot de informatiebeveiliging van de meldkamervoorzieningen via het beleids- en bestedingsplan kunnen aandragen (**lid 4**).

Gelet op de rol die zowel het Bestuurlijk Meldkamer Beraad als het Strategisch Meldkamer Beraad via het beleids- en bestedingsplan hebben op de informatiebeveiliging van de meldkamervoorzieningen, zullen in deze gremia ook de in-control verklaringen (ICV) van de beheerder en hoofdgebruikers worden besproken (**lid 5**). De BIO hanteert risicomanagement, aan de hand van de *Plan-DO-Check-Act-cyclus,* als uitgangspunt, waarbij de risicoanalyse en de ICV belangrijke instrumenten zijn. In het informatiebeveiligingsbeleid meldkamervoorzieningen wordt nader omschreven wat de ICV zal omvatten. De uitkomst van de ICV's, of de analyses horend bij het risicomanagementproces, hebben direct weerslag op het beleid en beheer van de meldkamers. Het Bestuurlijk en Strategisch Meldkamer Beraad zijn zodoende de meest geschikte gremia om deze onderwerpen te agenderen en te bespreken.

Het Bestuurlijk Meldkamer Beraad krijgt daarnaast, horende het advies van het Strategisch Meldkamer Beraad, de mogelijkheid om onderzoek te laten uitvoeren naar de werking van het informatiebeveiligingsbeleid. Het Bestuurlijk Meldkamer Beraad en Strategisch Meldkamer Beraad stellen wijzigingen in het informatiebeveiligingsbeleid vast. Bij een dergelijke taak moet ook de mogelijkheid gegeven worden de werking van het informatiebeveiligingsbeleid te toetsen (**lid 6**).

Als partijen bij beslispunten niet tot overeenstemming komen, kunnen zij het beslispunt escaleren tot op het hoogste besturingsniveau, het Bestuurlijk Meldkamer Beraad. Alle partijen moeten daarbij, volgens de toelichting van de Regeling hoofdlijnen beleid en beheer meldkamers, aangeven waarom zij wel of niet kunnen instemmen met het beslispunt.

Gelet op de specifieke taken die aan het SMB worden toebedeeld rondom het informatiebeveiligingsbeleid van de meldkamervoorzieningen, kan het SMB hiervoor een hulpstructuur inrichten (**lid 7**), waarin de beheerder en hoofdgebruikers zijn vertegenwoordigd, en dat bijdraagt aan de samenwerking en voorbereiding voor de in het Strategisch Meldkamer Beraad geagendeerde onderwerpen rondom de informatiebeveiliging van de meldkamervoorzieningen.

Artikel 4

Het strategisch kader heeft uitsluitend betrekking op de meldkamervoorzieningen die op de meldkamers gebruikt worden door de hoofdgebruikers bij de uitvoering van hun meldkamerfunctie én die in beheer zijn bij de Landelijke Meldkamer Samenwerking (hierna: beheerder), gepositioneerd bij de Nationale politie. De beheerder organiseert, met en voor de hoofdgebruikers, een landelijk beheerd, 24/7 bereik- en beschikbaar netwerk van tien operationeel en technisch met elkaar verbonden meldkamers waarop de brandweer, politie, ambulance en Defensie / Koninklijke Marechaussee hun meldkamerfuncties (gezamenlijk) kunnen uitoefenen. De beheerder is verantwoordelijk voor de instandhouding en beschikbaarheid van de meldkamervoorzieningen.

De beheerder heeft eigen taken en verantwoordelijkheden die horen bij het zijn van een beheerder van meldkamervoorzieningen. De beheerder dient voor zijn eigen taken en binnen de eigen beheerorganisatie het strategisch kader en informatiebeveiligingsbeleid meldkamervoorzieningen te implementeren, uit te voeren en te monitoren (**lid 1**). Daarnaast rolt de beheerder een risicomanagementproces uit, waar het uitvoeren van risicoanalyses onderdeel van is. De risicoanalyses zien niet alleen op het voldoen aan de normen in de BIO, maar zien specifiek ook op het vastgestelde Basis Beveiligingsniveau van een meldkamervoorziening. Zo kan, bijvoorbeeld, het Basis Beveiligingsniveau van een meldkamervoorziening op een hoger niveau worden vastgesteld dan het huidige BBN2. Indien dit het geval is dient een nadere risicoanalyse te worden uitgevoerd om te bezien welke maatregelen – aanvullend op de maatregelen vanuit de BIO – dienen te worden geïmplementeerd om risico's op bijvoorbeeld statelijke actoren te mitigeren. Gelet op de nauwe samenwerking met de hoofdgebruikers, zal de beheerder de hoofdgebruikers hierbij betrekken en consulteren (**lid 2**). Dit is een nauwere samenwerking dan wanneer de beheerder aan het einde van het traject uitsluitend de uitkomsten met de hoofdgebruikers afstemt.

Voor de beheerder is verder een faciliterende rol voorzien ten opzichte van de hoofdgebruikers als het gaat om de vaststelling en wijziging van het informatiebeveiligingsbeleid meldkamervoorzieningen (**lid 3**). De hoofdgebruikers zijn zelf verantwoordelijk voor het gebruik van de meldkamervoorzieningen binnen hun eigen organisatie. Als spin in het web is de beheerder echter in positie om op operationeel niveau het gemeenschappelijke karakter van het netwerk te bewaken waar die gedeelde verantwoordelijkheid op bestuurlijk niveau wordt vormgegeven in zowel het bestuurlijk als het strategisch meldkamerberaad. De beheerder bereidt de besluitvorming voor, maar de hoofdgebruikers leveren in de hoofdzaak de inhoud, en de beheerder neemt het initiatief tot wijziging, maar kan dat (ook) doen als een hoofdgebruiker daartoe een noodzaak ziet.

Tot slot wordt in **lid 4** van dit artikel de verantwoordelijkheid voor het monitoren van de naleving van het informatiebeveiligingsbeleid binnen de eigen beheerorganisatie neergelegd. In **lid 5** komt de verplichting tot het jaarlijks opstellen van een in-control verklaring (ICV) terug. De BIO beschrijft de risicoanalyse en de ICV als belangrijke instrumenten om het risicomanagement in te vullen. In het informatiebeveiligingsbeleid meldkamervoorzieningen wordt nader omschreven wat de ICV zal omvatten. De ICV van de beheerder is uitsluitend gericht op de beheerorganisatie.

Artikel 5

De term hoofdgebruikers en medegebruiker zijn afkomstig uit de Regeling hoofdlijnen beleid en beheer meldkamers en het kader Medegebruik (vastgesteld door het Bestuurlijk Meldkamer Beraad op 7 december 2021). In het kader van Medegebruik zijn vier hoofdgebruikers van de meldkamervoorzieningen aangewezen. Dit betreft politie, ambulance, brandweer en de Koninklijke marechaussee (voor de voorziening spoedrespons – C2000 – is niet de Koninklijke Marechaussee de hoofdgebruiker, maar Defensie). De hoofdgebruikers maken gebruik van de meldkamervoorzieningen bij het uitvoeren van hun wettelijke meldkamerfunctie. Het kan voorkomen dat een andere gebruiker dan de hoofdgebruikers een belang heeft om gebruik te maken van meldkamervoorzieningen, deze gebruiker wordt een medegebruiker genoemd[2].

Er is voor gekozen de hoofdgebruikers een grotere rol te geven bij het invullen van het informatiebeveiligingsbeleid meldkamervoorzieningen. Zo is getracht meer ruimte te bieden voor informatiebeveiligingsbeleid dat past bij de operationele werkelijkheid. De hoofdgebruikers zijn dan ook zelf verantwoordelijk voor het inrichten van een risicomanagementproces voor de door hem gebruikte meldkamervoorzieningen, conform de normen van de BIO, en in het bijzonder het bepaalde Basis Beveiligingsniveau. De risicoanalyses zien niet alleen op het voldoen aan de normen in de BIO, maar zien specifiek ook op het vastgestelde Basis Beveiligingsniveau van een meldkamervoorziening. Zo kan, bijvoorbeeld, het Basis Beveiligingsniveau van een meldkamervoorziening op een hoger niveau worden vastgesteld dan het huidige BBN2. Indien dit het geval is dient een nadere risicoanalyse te worden uitgevoerd om te bezien welke maatregelen – aanvullend op de maatregelen vanuit de BIO – dienen te worden geïmplementeerd om aanvullende risico's te mitigeren. Elke hoofdgebruiker is verantwoordelijk voor het implementeren en naleven van het informatiebeveiligingsbeleid meldkamervoorzieningen binnen de eigen organisatie en het monitoren daarvan (**lid 1, lid 2 en lid 3**). Vanwege deze verantwoordelijkheid bij de hoofdgebruikers is een extra laag onder de multidisciplinaire sturingslijn uit de Regeling hoofdlijnen beleid en beheer meldkamers toegevoegd door van de hoofdgebruikers te vragen een in-control verklaring (ICV) af te geven, die vervolgens tezamen met de ICV's van de andere hoofdgebruikers en de beheerder worden voorgelegd aan het Strategisch Meldkamer Beraad en Bestuurlijk Meldkamer Beraad. Zo wordt voorkomen dat rechtstreeks wordt ingegrepen in de operatie en dus de eigen verantwoordelijkheid van de hoofdgebruikers (**lid 5**).

Tot slot wordt in dit artikel ook de verantwoordelijkheid van de hoofdgebruiker voor het implementeren en naleven van (de relevante onderdelen van) het informatiebeveiligingsbeleid door de onder hem vallende medegebruikers benoemd (**lid 4**). De medegebruiker dient de voor hem verantwoordelijke hoofdgebruiker te rapporteren over de status van implementatie van het informatiebeveiligingsbeleid. Met medegebruikers die niet onder de verantwoordelijkheid vallen van een hoofdgebruiker (hiermee wordt gedoeld op de 'bijzondere gebruikers' in de beleidsregel toelating en gebruik C2000 door derden) worden afzonderlijk over hun wijze van rapporteren afspraken gemaakt. Hiermee wordt een link gemaakt met het kader Medegebruik en de Beleidsregel Toelating en gebruik C2000 door derden.

Artikel 6

In dit artikel wordt de taak van de Minister van Justitie en Veiligheid, als stelselverantwoordelijke en verantwoordelijke voor het strategisch kader, beschreven. De Minister dient minstens eens in de vijf jaar de werking van het strategisch kader te evalueren door middel van audits. Er is bewust voor gekozen om 'minstens eens in de vijf jaar' neer te zetten. Zodoende kan er vaker dan eens in de vijf jaar een audit plaatsvinden als daar behoefte aan is, bijvoorbeeld naar aanleiding van incidenten voortvloeiend uit de PDCA-cyclus.

Artikel 7

Dit artikel regelt dat het strategisch kader in werking treedt met ingang van de dag na datum van uitgifte van de Staatscourant waarin zij wordt geplaatst. Dit betekent dat het strategisch kader zo spoedig mogelijk in werking zal treden, waarbij mogelijk wordt afgeweken van de vaste verandermo-

[2] Onder de term medegebruiker wordt – naast de definitie die in het kader medegebruik is genoemd – ook de (tijdelijk) gelieerde en bijzondere gebruikers bedoeld, zoals omschreven in de Beleidsregels toelating en gebruik C2000 door derden.

menten voor de inwerkingtredingsdatum van een ministeriële regeling. Hiervoor is gekozen, zodat de betrokken partijen zo spoedig mogelijk aan de slag kunnen gaan met het implementatieplan voor het implementeren van het strategisch kader. Op deze wijze zullen zij zo snel als mogelijk in staat zijn om de eisen van het strategisch kader en het informatiebeveiligingsbeleid te kunnen naleven, wat noodzakelijk is voor de betrouwbaarheid en beschikbaarheid van de betreffende systemen.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius