STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 40208
16 december 2025

Besluit van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 14 december 2025, nr. 2025-0000042677 tot wijziging van het Besluit CIO-stelsel Rijksdienst 2021 (Besluit CIO-stelsel Rijksdienst 2026)

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties;

Handelend in overeenstemming met het gevoelen van de ministerraad;

Gelet op de artikelen 2, eerste lid, 3, eerste lid, en 6, eerste en tweede lid, van het Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst;

§ 1. Algemeen

Artikel 1. Definities

In dit besluit wordt verstaan onder:
a. *beveiligingsautoriteit:* beveiligingsautoriteit; bedoeld in artikel 3 van het Besluit BVA-stelsel Rijksdienst 2021;
b. *beveiligingsautoriteit Rijk:* beveiligingsautoriteit Rijk; bedoeld in artikel 7 van het Besluit BVA-stelsel Rijksdienst 2021;
c. *CIO:* Chief Information Officer bedoeld in artikel 3, eerste lid en artikel 16, eerste lid;
d. *CIO Rijk:* Chief Information Officer Rijk bedoeld in artikel 17, eerste lid;
e. *CISO:* Chief Information Security Officer bedoeld in artikel 6, eerste lid en artikel 16, vierde lid;
f. *CISO Rijk:* Chief Information Security Officer Rijk bedoeld in artikel 17, eerste lid;
g. *(C)DO:* (Chief) Data Officer bedoeld in artikel 9, eerste lid en artikel 10, eerste lid;
h. *(C)PO:* (Chief) Privacy Officer bedoeld in artikel 9, eerste lid en artikel 12, eerste lid;
i. *(C)TO:* (Chief) Technology Officer bedoeld in artikel 9, eerste lid en artikel 14, eerste lid;
j. *Coördinatiebesluit:* Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst;
k. *digitalisering:* geheel aan ontwikkelingen binnen de overheid en in de samenleving die te maken hebben met het toenemend gebruik van ICT, digitale informatie, data en informatiesystemen;
l. *grote ICT-component:* ICT-component vallend onder de definitie die in het Handboek portfoliomanagement Rijk wordt gegeven aan grote ICT-component;
m. *ICT:* Informatie- en communicatietechnologie;
n. *informatiebeveiliging:* proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen;
o. *informatiesysteem:* samenhangend geheel van gegevensverzamelingen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie;
p. *informatievoorziening:* geheel van mensen, middelen, informatiesystemen en maatregelen, gericht op de informatiebehoefte van een organisatie;
q. *portfoliomanagement:* proces van inventarisatie, registratie en actualisatie van wijzigingen in informatiesystemen, vastgelegd in een portfolio.

Artikel 2. Reikwijdte

1. Dit besluit geldt voor de rijksdienst, zijnde de kerndepartementen en de daaronder ressorterende dienstonderdelen inclusief de gevestigde diensten op Caribisch Nederland.

2. Bij de Rijksdienst Caribisch Nederland (RCN) is een CIO Rijksdienst Caribisch Nederland (CIO RCN) aangesteld, die rechtstreeks ressorteert onder de CIO Binnenlandse Zaken en Koninkrijksrelaties. De CIO RCN heeft dezelfde taken en verantwoordelijkheden als de departementale CIO bedoeld in artikel 3.

§ 2. CIO en CISO

Artikel 3. CIO-functie

1. De minister die belast is met de leiding van een ministerie draagt zorg voor de aanstelling van een departementale CIO die rechtstreeks ressorteert onder de secretaris-generaal van het ministerie.

2. De departementale CIO is belast met de ontwikkeling en coördinatie van het informatievoorzienings- en digitaliseringsbeleid en het zorgdragen voor de ontwikkeling en het beheer van de informatiesystemen van het ministerie conform dit beleid.

3. De departementale CIO is tevens belast met het inrichten van het CIO-stelsel voor het ministerie en de onder haar ressorterende dienstonderdelen.

4. De departementale CIO is lid van de bestuursraad van het ministerie.

5. Een CIO beschikt over een CIO-office.

6. Het CIO-office wordt zodanig ingericht dat over voldoende kennis en ervaring wordt beschikt om de taak, bedoeld in artikel 4 uit te voeren.

Artikel 4. Taken departementale CIO

De minister die belast is met de leiding van een ministerie draagt aan de departementale CIO met betrekking tot het ministerie in elk geval de volgende taken op:
a. het adviseren van het lijnmanagement en de minister over het beleid ten aanzien van informatievoorziening en digitalisering;
b. het adviseren van het lijnmanagement en de minister over de implicaties voor informatievoorziening en digitalisering van (voorgenomen) wet- en regelgeving, beleids- en uitvoeringstrajecten en investeringen;
c. het opstellen, beheren en zorgdragen voor de uitvoering van een meerjarig informatieplan voor het ministerie met een financiële paragraaf;
d. het richten op en stimuleren van digitale transformatie en technologisch gedreven innovatie binnen het ministerie door het investeren in een cultuur van kennisdeling en door het lerend vermogen op het gebied van digitalisering binnen het ministerie te bevorderen;
e. het met inachtneming van toepasselijke rijksbrede kaders en ICT-voorzieningen zorgdragen voor de ontwikkeling en coördinatie van informatievoorzieningsbeleid en digitaliseringsbeleid en de ontwikkeling en het beheer van de informatiesystemen van het ministerie;
f. het toezien op naleving van de kaders gesteld op grond van de artikelen 2 en 6 van het Coördinatiebesluit en het gevraagd en ongevraagd informeren en adviseren van het verantwoordelijk lijnmanagement en de CIO Rijk hierover;
g. het ontwikkelen en coördineren van integraal portfoliomanagement en levenscyclusmanagement om de samenhang tussen ICT-(door)ontwikkeling en ICT-beheer van het kerndepartement en dienstonderdelen te bewaken;
h. het gevraagd en ongevraagd adviseren en informeren van de CIO Rijk voor zover dit redelijkerwijs noodzakelijk is voor diens taakuitoefening, bedoeld in artikel 18;
i. het zorgdragen voor voldoende aandacht binnen het ministerie voor continue beheeractiviteit en verbetering van de ICT-infrastructuur inclusief de benodigde technologische vernieuwing en informatiebeveiliging;
j. het voeren van een solide informatiehuishouding waarbinnen de informatie duurzaam toegankelijk, vindbaar, juist, volledig en betrouwbaar bewaard wordt;
k. het uitvoeren van oordelen aangaande de beheersing, haalbaarheid, risico's en implicaties van alle voorgenomen en in uitvoering zijnde activiteiten met een grote ICT-component, conform de daarvoor geldende rijksbrede kwaliteitsnormen;
l. het aanmelden van activiteiten bij het Adviescollege ICT-toetsing, als bedoeld in artikel 7, eerste lid, onderdeel a, onder 2° van de Wet Adviescollege ICT-toetsing;
m. het uitvoeren van de taken met betrekking tot het (IV)beleidsterrein voor de eigen diensten die vallen onder het eigen ministerie;
n. het realiseren van interoperabiliteit tussen ministeries op tenminste uitwisselfunctionaliteiten en aansluiting op rijksbrede generieke voorzieningen en dienstverlening.

Artikel 5. Bevoegdheden departementale CIO

1. De departementale CIO kan, na overleg met de secretaris-generaal, de minister rechtstreeks informeren, indien zijn taakuitoefening op grond van dit besluit daartoe aanleiding geeft.

2. De departementale CIO kan een CIO-oordeel of een externe kwaliteitstoets uitvoeren binnen alle fasen van projecten, programma's of activiteiten met een digitaliseringsaspect of ICT-component.

3. Voor het aanvangen van ICT-ontwikkelprojecten en onderhoudsactiviteiten met een grote ICT-component, die onder verantwoordelijkheid van het ministerie worden uitgevoerd, is een positief CIO-oordeel, of een beargumenteerde afwijking hiervan door de secretaris-generaal van het ministerie, vereist.

4. De dienstonderdelen van het ministerie verstrekken de departementale CIO de informatie die noodzakelijk is voor de uitoefening van zijn taken op grond van dit besluit.

Artikel 6. Departementale CISO

1. De minister die belast is met de leiding van een ministerie draagt zorg voor de aanstelling van een departementale CISO die rechtstreeks ressorteert onder de CIO van het ministerie.

2. De departementale CISO is belast met de ontwikkeling en coördinatie van het departementale informatiebeveiligingsbeleid, bedoeld in artikel 3 van het Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007 en artikel 3 van het Besluit Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie 2025 en het ondersteunen van het verantwoordelijk lijnmanagement bij de implementatie en naleving hiervan.

Artikel 7. Taken departementale CISO

De minister die belast is met de leiding van een ministerie draagt aan de departementale CISO ten aanzien van digitalisering en informatievoorziening, met betrekking tot het ministerie, de taak op tot:

a. het ontwikkelen en coördineren van departementaal informatiebeveiligingsbeleid en -kaders en het ondersteunen van de implementatie en naleving hiervan;
b. het zorgdragen voor het departementale informatiebeveiligingsbeleid als onderdeel van het departementale digitaliserings- en informatievoorzieningsbeleid, bedoeld in artikel 4, onder e;
c. het ontwikkelen en actueel houden van een departementaal risicobeeld met betrekking tot informatiebeveiliging;
d. het bijdragen aan het opstellen en beheren van het meerjarig informatieplan voor het ministerie, bedoeld in artikel 4, onder c, met betrekking tot de departementale informatiebeveiliging;
e. het bijdragen aan het opstellen van het rijksbrede informatiebeveiligingsbeleid, het risicobeeld en het calamiteitenplan, bedoeld in artikel 20, onder a, c en j, en de rijksbrede strategie, bedoeld in artikel 18, onder a, en aan het integrale beveiligingsbeleid, de risicoanalyse en het calamiteitenplan, bedoeld in artikel 4, eerste, derde en zesde lid, van het Besluit BVA-stelsel Rijksdienst 2021, met betrekking tot de departementale informatiebeveiliging;
f. het gevraagd en ongevraagd adviseren van de departementale CIO, het verantwoordelijk lijnmanagement en CISO's van dienstonderdelen over de informatiebeveiliging en de risico's daarvoor van (voorgenomen) wet- en regelgeving, investeringen, beleids- en uitvoeringstrajecten, informatieprocessen en informatiesystemen;
g. het gevraagd en ongevraagd adviseren en informeren van de CISO Rijk voor zover dit redelijkerwijs noodzakelijk is voor diens taakuitoefening, bedoeld in artikel 20, en van de departementale beveiligingsautoriteit ten behoeve van diens taakuitoefening op grond van het bepaalde in het Besluit BVA-stelsel Rijksdienst 2021;
h. het monitoren en controleren van het informatiebeveiligingsbewustzijn binnen het ministerie, het adviseren van het kerndepartement en dienstonderdelen hierover en het zorgdragen voor het vergroten van het bewustzijn over informatiebeveiliging binnen het ministerie;
i. het onderhouden van relaties met de inlichtingen- en veiligheidsdiensten, het Nationaal Cyber Security Centrum en de Nationale Coördinator Terrorismebestrijding en Veiligheid aangaande dreigingen die verband houden met de informatiebeveiliging van het departement;
j. het ontwikkelen en coördineren van informatiebeveiligingsactiviteiten, -projecten en het zorgdragen voor een projectportfolio voor informatiebeveiliging;
k. het bijdragen aan CIO-oordelen en kwaliteitstoetsen als bedoeld in artikel 5, tweede lid, met betrekking tot informatiebeveiliging;
l. het binnen het ministerie coördineren van onderzoeken van de Auditdienst Rijk, Algemene Rekenkamer, Adviescollege ICT-toetsing en eventueel Autoriteit Persoonsgegevens naar het niveau van de naleving van het betreffende beleidsgebied;
m. het monitoren en signaleren van afwijkingen van artikel 41, eerste lid, van de Kaderwet zelfstandige bestuursorganen en het informeren hierover van de secretaris-generaal als eigenaar van een zelfstandig bestuursorgaan.

Artikel 8. Bevoegdheden departementale CISO

1. De departementale CISO kan de secretaris-generaal en het verantwoordelijk lijnmanagement van het ministerie rechtstreeks informeren, indien zijn taakuitoefening op grond van dit besluit en de ernst van het geconstateerde feit daartoe een acute aanleiding geeft. Indien vooroverleg met de CIO en de beveiligingsautoriteit niet mogelijk is, worden beiden zo spoedig mogelijk achteraf geïnformeerd.

2. De dienstonderdelen van het ministerie verstrekken de departementale CISO gevraagd en ongevraagd de informatie die noodzakelijk is voor de uitoefening van zijn taken.

3. De departementale CISO kan namens de secretaris-generaal en de departementale CIO aanwijzingen geven met betrekking tot informatieprocessen in het geval van een, mogelijke, ernstige en acute inbreuk op de beveiliging van informatiesystemen. De CISO laat onverwijld maatregelen treffen om zo veel mogelijk de beveiliging te laten herstellen en verdere schade te laten beperken.

4. De departementale CISO kan namens de secretaris-generaal en de departementale CIO en in afstemming met de beveiligingsautoriteit van het ministerie, aanwijzingen geven aan iedere ambtenaar, externe medewerkers en bezoekers, voor zover dat noodzakelijk is voor de uitvoering van het departementale informatiebeveiligingsbeleid en de naleving van de informatiebeveiligingsvoorschriften.

Artikel 9. Departementale (C)DO, (C)PO en (C)TO

1. Naast de benoemde CIO, CISO, CIO Rijk en CISO Rijk kunnen de ministeries de volgende rollen invullen:
   – (Chief) Data Officer (C)DO)
   – (Chief) Privacy Officer (C)PO)
   – (Chief) Technology Officer (C)TO)

2. Het staat de ministeries vrij om deze rollen als afzonderlijke functies binnen hun organisatiestructuur te formaliseren, rekening houdend met de specifieke behoeften en vereisten van hun operationele omgeving.

3. Indien de aard en het belang van de rol binnen het ministerie dit rechtvaardigen, kan aan de aanduiding van de rol het voorvoegsel ‘Chief’ worden toegevoegd, waarmee de status en verantwoordelijkheid van de functie worden benadrukt. Dit resulteert in de volgende titels:
   – Chief Data Officer (CDO)
   – Chief Privacy Officer (CPO)
   – Chief Technology Officer (CTO)

4. De departementale (C)DO, (C)PO en (C)TO zijn een tweedelijnsfunctie en ressorteren rechtstreeks onder de departementale CIO. Deze tweedelijnsfunctie gaat over adviseren, kaderstellen en monitoren.

5. De departementale CIO is verantwoordelijk voor de functionele aansturing alsmede voor de toewijzing van taken en verantwoordelijkheden.

Artikel 10. Taken departementale (Chief) Data Officer

De departementale (C)DO ressorteert onder de departementale CIO. De CIO kan de departementale (C)DO de volgende taken toewijzen:

a. het ontwikkelen en coördineren van een gegevensstrategie die richting geeft aan het gegevens en algoritmebeleid en integraliteit borgt van het gegevens-, algoritme- en Artificial Intelligence (AI)-beleid;
b. het zorgdragen voor het opstellen, beheren en monitoren van de uitvoering van het gegevens-, algoritme- en AI-beleid. Dit beleid omvat de volgende classificatie: gegevenstyperingsbeleid, gegevenskwaliteitsbeleid, gegevens- en algoritmegebruiksbeleid en gegevensdelingsbeleid;
c. het gevraagd en ongevraagd adviseren van de departementale CIO en het verantwoordelijk lijnmanagement in lijn met het verkregen mandaat en (C)DO’s van dienstonderdelen over gegevens-, algoritme- en AI-vraagstukken in onder andere (voorgenomen) wet- en regelgeving, investeringen, beleids- en uitvoeringstrajecten, informatieprocessen en informatiesystemen, CIO-oordelen en kwaliteitstoetsen;
d. het invullen van de randvoorwaarden voor en het onderkennen van de mogelijkheden van waardecreatie als ook het datagedreven werken. Dat houdt onder andere in het ontwikkelen, stimuleren of coördineren van activiteiten en projecten om dit kunnen te realiseren door onder

andere te investeren in gegevenscultuur en vaardigheden die nodig zijn om gegevens effectief te begrijpen, interpreteren en te gebruiken;
e. het monitoren van de uitvoering van assessments bij de inzet van algoritmes, zoals het Impact Assessment voor Mensenrechten (IAMA) en een AI impactassessment (AIIA) in afstemming of samenwerking met de (C)PO;
f. het opstellen van het beleid in diens beleidsgebied (te weten de visie, kaders, indicatoren, strategie en governance) voor het ministerie, de inrichting van het stelsel daarvan binnen het departement en het monitoren van de werking binnen de organisatieonderdelen;
g. het monitoren van de toepassing door de organisatie van de kaders op diens beleidsgebied. Het inrichten van een PDCA-cyclus voor de monitoring van de stand van zaken van de naleving van wet- en regelgeving en beleid bij alle organisatieonderdelen op diens beleidsgebied;
h. het zoeken van afstemming en samenwerking met de (C)xO's of specialisten van onder andere de vakgebieden: privacy, gegevens, informatiehuishouding, beveiliging, open source, open standaarden, technologie en duurzame toegankelijkheid en digitale toegankelijkheid;
i. het adviseren over en monitoren van de naleving van (internationale) wet- en regelgeving op het betreffende beleidsgebied om bij te dragen aan het realiseren van maatschappelijke opgaven;
j. het coördineren van kennisdeling en bewustwording op het betreffende beleidsgebied met daarbij specifiek oog voor het ethische, handelen in lijn met wet- en regelgeving op het betreffende beleidsgebied en het bijdragen aan het vergroten van het noodzakelijke bewustzijn binnen het ministerie of organisatieonderdeel;
k. het adviseren van betreffende beleidsgebied-professionals en het management van dienstonderdelen bij disputen en/of conflicterende belangen tussen verschillende dienstonderdelen rondom vraagstukken op het betreffende beleidsgebied;
l. het monitoren van de juiste afhandeling en juiste registratie in registers van het betreffende beleidsgebied bij incidenten of regulier gebruik waar dat verplicht of gewenst is;
m. het bijdragen aan het opstellen van rijksbreed beleid in samenwerking met de CIO Rijk;
n. het gevraagd en ongevraagd adviseren en informeren van de CIO Rijk voor zover dit redelijkerwijs noodzakelijk is;
o. het binnen het ministerie coördineren van onderzoeken van de Auditdienst Rijk, Algemene Rekenkamer, Adviescollege ICT-toetsing en eventueel Autoriteit Persoonsgegevens naar het niveau van de naleving van het betreffende beleidsgebied;
p. het op verzoek van de CIO bijdragen aan CIO-oordelen en kwaliteitstoetsen.

Artikel 11. Bevoegdheden departementale (Chief) Data Officer

1. De (C)DO handelt binnen het mandaat zoals dat is verstrekt door de CIO.

2. De (C)DO kan gevraagd en ongevraagd adviseren over het beleidsgebied van de (C)DO.

3. De (C)DO kan uit hoofde van de departementale CIO informatie opvragen bij (C)xO's, CIO's en het verantwoordelijk management van de organisatie (onderdelen) om inzicht te verkrijgen in de stand van zaken met betrekking tot naleving van wet- en regelgeving en beleid binnen het beleidsgebied van de (C)DO.

4. De (C)DO kan de departementale CIO adviseren te escaleren naar secretaris-generaal of minister in het geval van, mogelijk, ernstig nalaten van de naleving van wetgeving, met als doel de inbreuk weg te nemen en schade te beperken.

Artikel 12. Taken departementale (Chief) Privacy Officer

De departementale (C)PO ressorteert onder de departementale CIO. De CIO kan de departementale (C)PO de volgende taken toewijzen:
a. het vertalen van en het bijdragen aan beleid gerelateerd aan de bescherming van privacy en persoonsgegevens;
b. het zorgdragen voor het opstellen beheren en monitoren van de uitvoering van het privacy- en persoonsgegevensbeschermingsbeleid;
c. het gevraagd en ongevraagd adviseren van de departementale CIO en het verantwoordelijk lijnmanagement en (C)PO's van dienstonderdelen over verwerking van persoonsgegevens in onder andere (voorgenomen) wet- en regelgeving, investeringen, beleids- en uitvoeringstrajecten, informatieprocessen en informatiesystemen, CIO-oordelen en kwaliteitstoetsen voor zover het niet individuele casuïstiek betreft;
d. het monitoren van de uitvoering van Data Protection Impact Assessments (DPIA's) en Data Transfer Impact Assessments (DTIA's) en assessments bij de inzet van algoritmes zoals het Impact Assessment voor Mensenrechten (IAMA) en een AI impactassessment (AIIA) in afstemming of samenwerking met de (C)DO functie;
e. het opstellen van het beleid in diens beleidsgebied (te weten de visie, kaders, indicatoren, strategie

en governance) voor het ministerie, de inrichting van het stelsel daarvan binnen het departement en het monitoren van de werking binnen de organisatieonderdelen;
f. het monitoren van de toepassing door de organisatie van de kaders op diens beleidsgebied. Het inrichten van een PDCA-cyclus voor de monitoring van de stand van zaken van de naleving van wet- en regelgeving en beleid bij alle organisatieonderdelen op diens beleidsgebied;
g. het zoeken van afstemming en samenwerking met de (C)xO's of specialisten van onder andere de vakgebieden: privacy, gegevens, informatiehuishouding, beveiliging, open source, open standaarden, technologie en duurzame toegankelijkheid en digitale toegankelijkheid;
h. het adviseren over en monitoren van de naleving van (internationale) wet- en regelgeving op het betreffende beleidsgebied om bij te dragen aan het realiseren van maatschappelijke opgaven;
i. het coördineren van kennisdeling en bewustwording op het betreffende beleidsgebied met daarbij specifiek oog voor het ethische, handelen in lijn met wet- en regelgeving op het betreffende beleidsgebied en het bijdragen aan het vergroten van het noodzakelijke bewustzijn binnen het ministerie of organisatieonderdeel;
j. het adviseren van betreffende beleidsgebied-professionals en het management van dienstonderdelen bij disputen en/of conflicterende belangen tussen verschillende dienstonderdelen rondom vraagstukken op het betreffende beleidsgebied;
k. het monitoren van de juiste afhandeling en juiste registratie in registers van het betreffende beleidsgebied bij incidenten of regulier gebruik waar dat verplicht of gewenst is;
l. het bijdragen aan het opstellen van rijksbreed beleid in samenwerking met de CIO Rijk;
m. het gevraagd en ongevraagd adviseren en informeren van de CIO Rijk voor zover dit redelijkerwijs noodzakelijk is;
n. het binnen het ministerie coördineren van onderzoeken van de Auditdienst Rijk, Algemene Rekenkamer, Adviescollege ICT-toetsing en eventueel Autoriteit Persoonsgegevens naar het niveau van de naleving van het betreffende beleidsgebied;
o. het op verzoek van de CIO bijdragen aan CIO-oordelen en kwaliteitstoetsen.

Artikel 13. Bevoegdheden departementale (Chief) Privacy Officer

1. De (C)PO handelt binnen het mandaat zoals dat is verstrekt door de CIO.

2. De (C)PO kan gevraagd en ongevraagd adviseren over het beleidsgebied van de (C)PO.

3. De (C)PO kan uit hoofde van de departementale CIO informatie opvragen bij (C)xO's, CIO's en het verantwoordelijk management van de organisatie (onderdelen) om inzicht te verkrijgen in de stand van zaken met betrekking tot naleving van wet- en regelgeving en beleid binnen het beleidsgebied van de (C)PO.

4. De (C)PO kan de departementale CIO adviseren te escaleren naar secretaris-generaal of minister in het geval van, mogelijk, ernstig nalaten van de naleving van wetgeving, met als doel de inbreuk weg te nemen en schade te beperken.

Artikel 14. Taken departementale (Chief) Technology Officer

De departementale (C)TO ressorteert onder de departementale CIO. De CIO kan de departementale (C)TO de volgende taken toewijzen:
a. het adviseren van de departementale CIO en op verzoek van de CIO het lijnmanagement over het gevoerde technologie- en innovatiebeleid;
b. het gevraagd en ongevraagd adviseren van de departementale CIO en het verantwoordelijk lijnmanagement en (C)TO's van dienstonderdelen over de technologische innovatie, investeringen, beleids- en uitvoeringstrajecten, informatieprocessen en informatiesystemen, CIO-oordelen en kwaliteitstoetsen voor zover het niet individuele casuïstiek betreft;
c. het mede-ontwikkelen en mede-uitvoeren van de departementale strategie samen met de departementale CIO, CISO, (C)DO en (C)PO, met de nadruk op bedrijfscontinuïteit en lifecyclemanagement;
d. het mede ontwikkelen en uitvoeren van meerjarenplannen en een digitale visie voor het IT-landschap van de organisatie en het bijdragen op de totstandkoming van de IV-portfolio;
e. het onderhouden van strategische relaties met ICT-leveranciers in de markt en relevante marktpartijen en diensten aangaande het IV-beleid van het departement;
f. het bijdragen aan de technologische kennis en vaardigheden door technologische kennisuitwisseling in het departement te faciliteren;
g. het periodiek informeren en rapporteren aan de departementale CIO over het gevoerde technologie- en innovatiebeleid;
h. het opstellen van het beleid in diens beleidsgebied (te weten de visie, kaders, indicatoren, strategie en governance) voor het ministerie, de inrichting van het stelsel daarvan binnen het departement en het monitoren van de werking binnen de organisatieonderdelen;

i. het monitoren van de toepassing door de organisatie van de kaders op diens beleidsgebied. Het inrichten van een PDCA-cyclus voor de monitoring van de stand van zaken van de naleving van wet- en regelgeving en beleid bij alle organisatieonderdelen op diens beleidsgebied;
j. het zoeken van afstemming en samenwerking met de (C)xO's of specialisten van onder andere de vakgebieden: privacy, gegevens, informatiehuishouding, beveiliging, open source, open standaarden, technologie en duurzame toegankelijkheid en digitale toegankelijkheid;
k. het adviseren over en monitoren van de naleving van (internationale) wet- en regelgeving op het betreffende beleidsgebied om bij te dragen aan het realiseren van maatschappelijke opgaven;
l. het coördineren van kennisdeling en bewustwording op het betreffende beleidsgebied met daarbij specifiek oog voor het ethische, handelen in lijn met wet- en regelgeving op het betreffende beleidsgebied en het bijdragen aan het vergroten van het noodzakelijke bewustzijn binnen het ministerie of organisatieonderdeel;
m. het adviseren van betreffende beleidsgebied-professionals en het management van dienstonderdelen bij disputen en/of conflicterende belangen tussen verschillende dienstonderdelen rondom vraagstukken op het betreffende beleidsgebied;
n. het monitoren van de juiste afhandeling en juiste registratie in registers van het betreffende beleidsgebied bij incidenten of regulier gebruik waar dat verplicht of gewenst is;
o. het bijdragen aan het opstellen van rijksbreed beleid in samenwerking met de CIO Rijk;
p. het gevraagd en ongevraagd adviseren en informeren van de CIO Rijk voor zover dit redelijkerwijs noodzakelijk is;
q. het binnen het ministerie coördineren van onderzoeken van de Auditdienst Rijk, Algemene Rekenkamer, Adviescollege ICT-toetsing en eventueel Autoriteit Persoonsgegevens naar het niveau van de naleving van het betreffende beleidsgebied;
r. het op verzoek van de CIO bijdragen aan CIO-oordelen en kwaliteitstoetsen.

Artikel 15. Bevoegdheden departementale (Chief) Technology Officer

1. De (C)TO handelt binnen het mandaat zoals dat is verstrekt door de CIO.

2. De (C)TO kan gevraagd en ongevraagd adviseren over het beleidsgebied van de (C)TO.

3. De (C)TO kan uit hoofde van de departementale CIO informatie opvragen bij (C)xO's, CIO's en het verantwoordelijk management van de organisatie (onderdelen) om inzicht te verkrijgen in de stand van zaken met betrekking tot naleving van wet- en regelgeving en beleid binnen het beleidsgebied van de (C)TO.

4. De (C)TO kan de departementale CIO adviseren te escaleren naar secretaris-generaal of minister in het geval van, mogelijk, ernstig nalaten van de naleving van wetgeving, met als doel de inbreuk weg te nemen en schade te beperken.

Artikel 16. Departementaal CIO-stelsel

1. De minister die belast is met de leiding van een ministerie draagt er zorg voor dat voor dienstonderdelen met een substantieel portfolio van informatiesystemen een eigen CIO wordt aangesteld.

2. De CIO van een dienstonderdeel is belast met de ontwikkeling en de coördinatie van het informatievoorzienings- en digitaliseringsbeleid voor het dienstonderdeel en het zorgdragen voor de ontwikkeling en het beheer van de informatiesystemen van het dienstonderdeel conform dit beleid. De taken en bevoegdheden van de CIO van een dienstonderdeel zijn een afgeleide van de taken en bevoegdheden van de departementale CIO, bedoeld in de artikelen 4 en 5.

3. De CIO van een dienstonderdeel maakt deel uit van de hoogste ambtelijke leiding van het betreffende dienstonderdeel.

4. De minister die belast is met de leiding van een ministerie draagt er zorg voor dat voor dienstonderdelen met een substantieel portfolio van informatiesystemen een CISO wordt aangesteld, ressorterend onder de CIO van het dienstonderdeel.

5. De CISO van een dienstonderdeel is belast met het informatiebeveiligingsbeleid, bedoeld in artikel 3 van het Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007 en artikel 3 van het Besluit Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie 2025, voor zover dit betrekking heeft op het dienstonderdeel. De taken en bevoegdheden van de CISO van een dienstonderdeel zijn een afgeleide van de taken en bevoegdheden van de departementale CISO, bedoeld in de artikelen 7 en 8.

6. Een CIO en een CISO van een dienstonderdeel maken onderdeel uit van het departementale

CIO-stelsel. Hetzelfde geldt voor de (C)DO, (C)PO en (C)TO wanneer deze rollen zijn ingevuld.

§ 3. CIO Rijk en CISO Rijk

Artikel 17. CIO Rijk en CISO Rijk

1. De Minister van Binnenlandse Zaken en Koninkrijksrelaties stelt een Chief Information Officer Rijk en een Chief Information Security Officer Rijk aan.

2. De CIO Rijk is belast met de ontwikkeling en coördinatie van het rijksbrede informatievoorzienings- en digitaliseringsbeleid en draagt zorg voor de ontwikkeling en het beheer van de ICT-voorzieningen en informatiesystemen, bedoeld in artikel 2, eerste lid onder b, van het Coördinatiebesluit.

3. De CISO Rijk is belast met de coördinatie van de maatregelen en het beleid voor de informatiebeveiliging voor zover deze betrekking hebben op de rijksdienst en ressorteert onder de CIO Rijk.

Artikel 18. Taken CIO Rijk

De Minister van Binnenlandse Zaken en Koninkrijksrelaties draagt aan de CIO Rijk met betrekking tot de rijksdienst de taak op tot:

a. richten op en stimuleren van digitale transformatie en technologisch gedreven innovatie, door het investeren in een cultuur van kennisdeling en door het lerend vermogen op het gebied van digitalisering te bevorderen;
b. het adviseren van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en het lijnmanagement van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties over de gevolgen voor het rijksbrede digitaliserings- en informatievoorzieningsbeleid, de rijksbrede informatieprocessen en informatiesystemen van onder andere (voorgenomen) wet- en regelgeving, beleid, uitvoeringstrajecten en investeringen voor zover deze betrekking hebben op de rijksdienst;
c. het coördineren van het CIO-stelsel binnen de Rijksdienst;
d. het ontwikkelen, coördineren en monitoren van de implementatie van het rijksbrede digitaliserings- en informatievoorzieningsbeleid;
e. het ontwikkelen en beheren van kaders zoals bedoeld in artikel 2, eerste lid, en 6, tweede lid, van het Coördinatiebesluit, met betrekking tot informatiesystemen van de ministeries;
f. het beoordelen van op grond van de in artikel 6, eerste lid, van het Coördinatiebesluit ontvangen informatie voor eventuele aanscherping van de kaders, bedoeld in onderdeel e, en ter bevordering van het lerend vermogen op het gebied van digitalisering binnen de rijksdienst;
g. het voorbereiden van de jaarrapportage over de digitalisering, informatievoorziening en informatiesystemen binnen de rijksdienst;
h. het toezien op de naleving van de op grond van artikelen 2, eerste lid, en 6, tweede lid, van het Coördinatiebesluit gestelde kaders over de informatiesystemen van de ministeries en de wijze waarop de gegevens over de informatiesystemen worden verstrekt; en
i. het toezien op de kwaliteitsaspecten van de informatieplannen, bedoeld in artikel 4, onder c, aan vastgestelde kwaliteitsnormen en het rapporteren hierover aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties;
j. het jaarlijks voeren van individuele departementale gesprekken met de departementale CIO's en de leden van het CIO-beraad. Door de CIO Rijk wordt hiervan een verslag en actielijst opgesteld, deze wordt gedeeld met de departementale CIO en het lid van het CIO-beraad;
k. het ontwikkelen van een meerjarige strategie op het gebied van digitalisering en informatievoorziening en het coördineren en monitoren van de uitvoering daarvan en over de voortgang verslag uitbrengen aan het CIO-beraad;
l. het coördineren van en toezien op interoperabiliteit tussen ministeries op tenminste uitwissel functionaliteiten en aansluiting op rijksbrede generieke voorzieningen en dienstverlening.

Artikel 19. Bevoegdheden CIO Rijk

1. De CIO Rijk kan, na overleg met de secretaris-generaal van Binnenlandse Zaken en Koninkrijksrelaties, de Minister van Binnenlandse Zaken en Koninkrijksrelaties rechtstreeks informeren, indien zijn taakuitoefening op grond van dit besluit daartoe aanleiding geeft.

2. In onderlinge samenhang gelezen geven artikel 11 van het Organisatiebesluit BZK 2023 en artikel 5.1 en artikel 7.1 van het Mandaatbesluit BZK 2023 de CIO Rijk het mandaat om namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties de kaders bedoeld in artikel 2, eerste lid, en artikel 6, tweede lid, van het Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst, na overleg met de ministers die het mede aangaat, vast te stellen.

3. De CIO Rijk voert namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties het overleg, bedoeld in artikel 3a van het Coördinatiebesluit.

Artikel 20. Taken CISO Rijk

De Minister van Binnenlandse Zaken en Koninkrijksrelaties draagt aan de CISO Rijk ten aanzien van digitalisering en informatievoorziening met betrekking tot de rijksdienst de taak op tot:

a. het ontwikkelen, coördineren en monitoren van de implementatie en naleving van rijksbreed informatiebeveiligingsbeleid en -kaders en de wijze waarop de gegevens over de informatiebeveiliging van informatiesystemen door de ministeries worden verstrekt;
b. het zorg dragen voor het rijksbrede informatiebeveiligingsbeleid als onderdeel van het rijksbrede digitaliserings- en informatievoorzieningsbeleid, bedoeld in artikel 18, onder d;
c. Het ontwikkelen en coördineren van het onderdeel informatiebeveiliging in de meerjarige strategie, bedoeld in artikel 18, onderdeel d;
d. het adviseren van de CIO Rijk en het lijnmanagement van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties over de informatiebeveiliging en de risico's daarvoor van (voorgenomen) wet- en regelgeving, investeringen, beleid, uitvoeringstrajecten, informatieprocessen en informatiesystemen voor zover deze betrekking hebben op de rijksdienst;
e. het gevraagd en ongevraagd uitbrengen van rijksbrede adviezen en verstrekken van informatie, inzake informatiebeveiliging en het risicomanagement daarvan;
f. het gevraagd en ongevraagd adviseren en informeren van de beveiligingsautoriteit Rijk ten behoeve van diens taakuitoefening op grond van het bepaalde in het Besluit BVA-stelsel Rijksdienst 2021;
g. het monitoren en controleren van het informatiebeveiligingsbewustzijn binnen de rijksdienst en het zorgdragen voor het vergroten van het bewustzijn over informatiebeveiliging binnen de rijksdienst;
h. het onderhouden van relaties met de inlichtingen- en veiligheidsdiensten, het Nationaal Cyber Security Centrum en de Nationale Coördinator Terrorismebestrijding en Veiligheid aangaande dreigingen die verband houden met de informatiebeveiliging van de rijksdienst;
i. het in samenwerking met de CISO's en beveiligingsautoriteit Rijk opstellen en actueel houden van het rijksbrede risicobeeld en calamiteitenplan met betrekking tot informatiebeveiliging;
j. het coördineren van de aanpak van rijksbrede informatiebeveiligingsincidenten en -calamiteiten.

Artikel 21. Bevoegdheden CISO Rijk

1. De CISO Rijk kan de secretaris-generaal van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het verantwoordelijk lijnmanagement van dat ministerie rechtstreeks informeren, indien zijn taakuitoefening op grond van dit besluit en de ernst van het geconstateerde feit daartoe een acute aanleiding geeft. Indien vooroverleg met de CIO Rijk en beveiligingsautoriteit Rijk niet mogelijk is, worden beiden zo spoedig als mogelijk achteraf geïnformeerd.

2. De CISO Rijk heeft een interdepartementale coördinatierol bij rijksbrede informatiebeveiligingsincidenten en -calamiteiten. De CISO Rijk kan, na afstemming met de betreffende departementale CISO, in het geval van een, mogelijke, ernstige, acute, departement-overstijgende inbreuk op de beveiliging van informatiesystemen of een risico daarop, namens de secretaris-generaal van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties:
   a. aanwijzingen geven aan iedere ambtenaar, externe medewerker en bezoeker met betrekking tot de informatieprocessen van ministeries;
   b. onverwijld maatregelen laten treffen om (zo veel mogelijk) de informatiebeveiliging te laten herstellen en verdere schade te laten beperken.

3. De CISO Rijk stemt onverwijld af met de CIO Rijk, de beveiligingsautoriteit Rijk en betrokken ministeries over een (mogelijke) inbreuk of het risico daarop en de genomen maatregelen, als bedoeld in het tweede lid, en heeft daarbij in afstemming met de departementale CISO's indien nodig direct toegang tot de secretarissen-generaal van ministeries.

4. De CISO Rijk kan de ministeries vragen informatie te verstrekken ten behoeve van het monitoren van de toepassing van de door het CIO-beraad, de CIO Rijk of CISO Rijk vastgestelde kaders, wet- en regelgeving en beleid op het gebied van informatiebeveiliging.

§ 4. CIO-beraad en Rijks ICT-dashboard

Artikel 22. CIO-beraad

1. Er is een CIO-beraad dat primair belast is met de rijksbrede coördinatie op informatievoorziening

en ICT. Het CIO-beraad ontwikkelt en implementeert een strategie voor de rijksdienst en bevordert digitalisering binnen de rijksdienst.

2. Het CIO-beraad wordt voorgezeten door de CIO Rijk.

3. Aan het CIO-beraad nemen ten minste de departementale CIO's als lid deel.

4. Het CIO-beraad stelt een Reglement CIO-beraad en Voorportalen vast waarin de voorwaarden voor deelname en wijze van vergaderen nader zijn uitgewerkt. Dit Reglement wordt minimaal tweejaarlijks geactualiseerd.

5. Het CIO-beraad kan één of meerdere voorportalen instellen. De werking van het CIO-beraad en de Voorportalen wordt beschreven in het Reglement CIO-beraad en Voorportalen.

Artikel 23. Rijks ICT-dashboard

1. Er is een Rijks ICT-dashboard.

2. Het Rijks ICT-dashboard bevat informatie over de staat van de informatievoorziening en digitalisering binnen de rijksdienst.

3. De CIO Rijk draagt zorg voor het beheer van het Rijks ICT-dashboard en het daarbinnen gehanteerde rapportagemodel.

4. De departementale CIO draagt zorg voor het periodiek actualiseren van het Rijks ICT-dashboard en de kwaliteit van de gegevens van zijn ministerie.

§ 5. Slotbepalingen

Artikel 24. Uitzonderingen

In overleg met de Minister van Binnenlandse Zaken en Koninkrijksrelaties kan op onderdelen worden afgeweken van het bepaalde in dit besluit, wanneer dit de effectiviteit van de met dit besluit beoogde doelen ten goede komt.

Artikel 25. Evaluatie

Dit besluit wordt drie jaar na inwerkingtreding geëvalueerd en vervolgens elke drie jaar.

Artikel 26. Inwerkingtreding

Dit besluit treedt in werking met ingang van 1 januari 2026.

Artikel 27. Citeertitel

Dit besluit wordt aangehaald als: Besluit CIO-stelsel Rijksdienst 2026.

Dit besluit zal met de toelichting in de Staatscourant worden geplaatst.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
E. van Marum

TOELICHTING

bij het Besluit CIO-stelsel Rijksdienst 2026

Algemeen deel

Aanleiding

Het CIO-stelsel binnen de rijksdienst bestaat sinds 2008. In dat jaar heeft het kabinet besloten een CIO bij elk ministerie in te stellen, omdat het bij kan dragen aan een betere positie van een minister in de besluitvorming over grote ICT-projecten. De Minister van Binnenlandse Zaken en Koninkrijksrelaties heeft namens het kabinet in een brief van 20 december 2019 aan de Tweede Kamer der Staten-Generaal bericht dat er een Besluit CIO-stelsel Rijksdienst zal komen. Het Besluit CIO-stelsel Rijksdienst 2021 (Stb. 2020, 62488) is het resultaat daarvan en biedt een solide juridische grondslag voor het CIO-stelsel.

In het besluit uit 2021 zijn de rollen, taken, verantwoordelijkheden en bevoegdheden van functionarissen binnen het CIO-stelsel inclusief de nieuw gecreëerde functie van Chief Information Security Officer Rijk (CISO Rijk), in goede samenhang geformaliseerd. Het besluit bevordert nog meer de samenwerking en coördinatie tussen rijksoverheidsinstanties waardoor efficiëntie en effectiviteit worden vergroot. Het stelsel zorgt voor een betere uitwisseling van informatie, bevordert transparantie en maakt het mogelijk om snel en flexibel in te spelen op veranderende behoeften en uitdagingen binnen de Rijksoverheid. Het besluit is ontworpen om de digitale transformatie van de Rijksoverheid te bevorderen en haar in staat te stellen een moderne en wendbare organisatie te worden.

Bij de huidige wijziging is een balans gevonden tussen de druk ten aanzien van lastenverlichting en de taakstelling op de bedrijfsvoering, de trend om te vereenvoudigen (complexiteitsreductie), de noodzakelijke professionalisering en standaardisatie en de behoefte om zaken efficiënter, doeltreffender en robuuster in te richten. Tevens is in het onderliggende Reglement de richting ingeslagen naar een meer integrale, opgavegerichte (en daarmee meer multidisciplinaire) manier van werken waardoor het CIO-beraad strategisch en efficiënt kan sturen op de digitaliseringsopgave die er rijksbreed ligt.

Artikel 25 van het besluit regelt dat er drie jaar na de inwerkingtreding van dat besluit, en vervolgens om de drie jaren, een evaluatie van dat besluit plaatsvindt. Volgens de toelichting komt hiermee ook het groeimodel van dat besluit tot uitdrukking en is daarmee op zichzelf ook een uiting van de digitale transformatie van de rijksdienst

Het geheel heeft geleid tot wijziging van het Besluit CIO-stelsel Rijksdienst 2021 welke recht doet aan de ontwikkelingen in het vakgebied informatievoorziening en de integrale en efficiënte sturing hierop inricht. Hierna wordt kort ingegaan op de rol van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, de CIO Rijk en de C-rollen. Daarna worden artikelsgewijs de wijzigingen toegelicht.

De rol van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de CIO Rijk

De rol van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en daarbinnen de CIO Rijk is gebaseerd op het 'Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst' in combinatie met het Organisatiebesluit en het Mandaatbesluit van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. In de artikelen 17, 18 en 19 wordt in het verlengde daarvan ingegaan op het mandaat, de taken en verantwoordelijkheden van de CIO Rijk. Hierbij hoort ook dat het CIO-beraad haar invloed kan inzetten op de strategische visie en realisatie van beleid binnen de Rijksdienst op het gebied van digitalisering, waar implicaties voor de maatschappij en samenleving aan de orde zijn. Denk bijvoorbeeld aan strategische advisering voor en het richtinggevend beïnvloeden van de politieke en bestuurlijke top.

De positionering van de C-rollen

Op departementaal niveau laat de ordening tussen de departementale CIO en de departementale C-rollen zich als volgt schetsen. De CIO is belast met de ontwikkeling en coördinatie van het informatievoorzienings- en digitaliseringbeleid van het departement en stuurt de andere C-rollen aan (in specifiek voorkomende situaties heeft de CISO een eigenstandige bevoegdheid, zie artikel 20 e.v.). De C-functies/-rollen leggen daarmee verantwoording af aan de CIO en de CIO is tevens verantwoordelijk voor de integraliteit. De CDO, CPO, CTO zijn rollen die eventueel als functie kunnen worden ingevuld. Het invullen is niet verplicht en de CDO, CPO en CTO kunnen indien gewenst ook worden gecombineerd, al dan niet met andere rollen. Het gebruik van de letter 'C' (Chief) is optioneel. Er is

daardoor ruimte om departementale keuzes te maken. Zie onder andere de artikelen 1 tot en met 5 en de artikelen 10, 12 en 14.

De C-functies/rollen zijn inhoudelijk. In sommige gevallen kunnen ze ook worden ingevuld door coördinerende specialisten die ervoor zorgen dat een bepaald aspect voldoende meegenomen wordt in de strategie, beleidsvorming, toezicht en uitvoering. Binnen het departement zijn de C-rollen dus (tweedelijns) adviseur en ze ontlasten de CIO die zich daardoor meer op strategische, fundamentele- en/of meer politiek-bestuurlijke vraagstukken met grote impact op de organisatie, de rijksdienst als geheel en de samenleving kan richten. De C-rollen overleggen binnen een departement met elkaar om te komen tot adviezen met een brede integrale afweging. De CIO blijft daarbij verantwoordelijk voor de integraliteit en zal in het geval van tegengestelde belangen een keuze maken (in relatie tot het IV-belang).

Interdepartementaal overleggen de C-functies/rollen met elkaar en wisselen kennis en informatie uit via de voorportalen van het CIO-beraad om te zorgen dat rijksbreed eenzelfde lijn wordt gevolgd en er synergie optreedt. Ook bereiden ze besluitvorming in het CIO-beraad voor.
Gezien de snelle ontwikkelingen in het vakgebied, en de huidige technologische en geopolitieke ontwikkelingen, is het de komende jaren noodzakelijk om expertise te hebben op de verschillende domeinen om de digitale transitie te realiseren. Naar de toekomst toe is er een gezonde waakzaamheid om kritisch te blijven op de omvang van de C-rollen in termen van efficiency, effectiviteit en integraliteit. Dit past bij de lijn waarlangs het CIO-stelsel zich de komende tijd verder zal ontwikkelen, het blijft immers een groeimodel.

Artikelsgewijze toelichting

Considerans

In de considerans is een verwijzing gemaakt naar artikel 6 eerste en tweede lid van het Coördinatiebesluit organisatie en bedrijfsvoeringrijksdienst 2011 (in plaats van alleen het tweede lid).

Artikel 1. (Definities)

In dit artikel zijn enkele definities toegevoegd.

Artikel 2. (Reikwijdte)

De CIO Rijksdienst Caribisch Nederland (CIO RCN) is onderdeel van het CIO-stelsel Rijksdienst. Hiërarchisch is de CIO Rijksdienst Caribisch Nederland onderdeel van de organisatiestructuur van de Rijksdienst Caribisch Nederland. Functioneel ressorteert de CIO RCN onder de CIO Binnenlandse Zaken en Koninkrijksrelaties. De taken en verantwoordelijkheden van de CIO Rijksdienst Caribisch Nederland worden vastgelegd in een mandaatregeling die door het CIO-beraad wordt bekrachtigd.

Artikel 3. (CIO-functie)

Geen wijzigingen.

Artikel 4. (Taken departementale CIO)

- Leden j, l, m en n zijn aangepast resp. toegevoegd. De leden m en n zijn rechtstreeks (integraal) overgenomen uit reeds door het CIO-beraad vastgestelde Tijdelijke Werkafspraken.
- In lid j wordt ingegaan op het belang van een solide informatiehuishouding.
- In lid l is de verwijzing naar het Instellingsbesluit Adviescollege ICT-toetsing vervangen door een verwijzing naar de Wet Adviescollege ICT-toetsing.
- In lid m is geëxpliciteerd dat de departementale CIO niet alleen verantwoordelijk is voor het kerndepartementen maar ook verantwoordelijkheid dragen voor het (IV)beleidsterrein voor de eigen diensten die vallen onder het eigen ministerie.
- In lid n is opgenomen dat het realiseren van interoperabiliteit tussen ministeries van belang is om eenheid, kwaliteit en efficiëntie van de uitvoering van het informatievoorzienings- en digitaliseringsbeleid te bevorderen, en dat de departementale CIO daarin een belangrijke rol vervult.

Artikel 5. (Bevoegdheden departementale CIO)

Geen wijzigingen.

Artikel 6. (Departementale CISO)

Geen wijzigingen.

Artikel 7. (Taken departementale CISO)

Aan artikel 7 is lid l toegevoegd waardoor dit lid zowel bij de CDO, CPO en CTO als de CISO is opgenomen.

Artikel 8. (Bevoegdheden departementale CISO)

Geen wijzigingen.

Artikel 9. (Departementale (C)DO, (C)PO en (C)TO)

Met de toevoeging van de (C)DO, (C)PO en (C)TO en de bijbehorende gremia in dit stelsel wordt een aantal inhoudelijke experts in positie gebracht om de departementale CIO's te adviseren over specifieke vraagstukken en om rijksbreed de slagkracht op het gebied van Privacy, Data en de inzet van technologie te vergroten. Door deze toevoeging worden de CIO's ontlast en ontstaat er op de agenda van het CIO-beraad ruimte voor strategische vraagstukken. Het staat de departementen vrij om deze posities in te vullen met (fulltime) functies of als rol (naast of als onderdeel van een andere functie).

Artikel 10. (Taken departementale (Chief) Data Officer)

Zie de toelichting bij artikel 9.

Artikel 11. (Bevoegdheden departementale (Chief) Data Officer)

Zie de toelichting bij artikel 9.

Artikel 12. (Taken departementale (Chief) Privacy Officer)

Zie de toelichting bij artikel 9.

Artikel 13. (Bevoegdheden departementale (Chief) Privacy Officer)

Zie de toelichting bij artikel 9.

Artikel 14. (Taken departementale (Chief) Technology Officer)

Zie de toelichting bij artikel 9.

Artikel 15. (Bevoegdheden departementale (Chief) Technology Officer)

Zie de toelichting bij artikel 9.

Artikel 16. (Departementaal CIO-stelsel)

Dit artikel is uitgebreid met de toevoeging van de (C)DO, (C)PO en (C)TO van een dienstonderdeel als onderdeel van het departementale CIO-stelsel, wanneer deze rollen of functies binnen een dienstonderdeel zijn ingevoerd.

Artikel 17. (CIO Rijk en CISO Rijk)

Kleine toevoeging bij lid 2: '... ICT-voorzieningen ...'.

Artikel 18. (Taken CIO Rijk)

- Lid d beschrijft de taak van de CIO Rijk om het rijksbrede digitaliserings- en informatievoorzieningsbeleid te ontwikkelen, te coördineren en de implementatie te monitoren.
- Lid j beschrijft dat de CIO Rijk jaarlijks gesprekken voert met de departementale CIO's en/of de leden van het CIO-beraad. Met deze gesprekken kan de CIO Rijk de voortgang bij departementen monitoren. Door de toevoeging kunnen ook aan het CIO-beraad deelnemende uitvoeringsorganisaties worden meegenomen in de jaargesprekken.
- Lid k beschrijft de taak van de CIO Rijk om een meerjarige strategie op het gebied van digitalise-

ring en informatievoorziening te ontwikkelen en de uitvoering daarvan te coördineren en monitoren. In deze strategie staan de gezamenlijke ambities en doelen van de CIO's van het rijk voor de informatievoorziening. Over de voortgang wordt verslag gedaan aan het CIO-beraad.
- Het voormalige lid I is vervallen.
- Het huidige lid I regelt de coördinatie op het realiseren van interoperabiliteit tussen ministeries, zoals bedoeld in artikel 4 lid I.

Artikel 19. (Bevoegdheden CIO Rijk)

- Lid 2 expliciteert de bevoegdheid van de CIO Rijk om kaders vast stellen. Het Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst spreekt van de Minister van Binnenlandse Zaken en Koninkrijksrelaties. Ten aanzien van de onderwerpen die behoren tot de portefeuille van de Staatssecretaris Digitalisering en Koninkrijksrelaties dient in het Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst voor 'de Minister van Binnenlandse Zaken en Koninkrijksrelaties te worden gelezen 'de Staatssecretaris Digitalisering en Koninkrijksrelaties'.
  Het Organisatiebesluit BZK 2023 en het Mandaatbesluit BZK 2023 moeten in onderlinge samenhang worden gelezen. In artikel 11 van het Organisatiebesluit BZK 2023 staat welke taken en aangelegenheden tot het DG Digitalisering en Overheidsorganisatie behoren. Vervolgens vloeit uit artikel 5.1 en artikel 7.1 het Mandaatbesluit BZK 2023 voort dat de dg Digitalisering en Overheidsorganisaties en de directeur CIO Rijk mandaat hebben om deze taken en aangelegenheden uit te voeren voor zover die het eigen werkterrein betreffen. Voor de volledigheid: mandaat betekent dat de mandaatgever, in dit geval de minister of staatssecretaris, zelf ook bevoegd blijft.
- Lid 3 verwijst naar artikel 3a Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst: het namens de Staat aangaan, wijzigen en beëindigen van de arbeidsovereenkomst met de Chief Information Officer van een ministerie geschiedt na overleg met Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties.

Artikel 20. (Taken CISO Rijk)

Geen wijzigingen.

Artikel 21. (Bevoegdheden CISO Rijk)

Artikel aangepast: lid 4 maakt duidelijk dat de CISO Rijk de informatie beschreven in het lid mag opvragen en ontvangen. In artikel 3 is het woord departementen op één plek vervangen door ministeries.

Artikel 22. (CIO-beraad)

Artikel aangepast: de uitwerking ten aanzien van de Voorportalen is verplaatst naar het onderliggende Reglement.

Artikel 23. (Rijks ICT-dashboard)

Geen wijzigingen.

Artikel 24. (Uitzonderingen)

Geen wijzigingen.

Artikel 25. (Evaluatie)

Geen wijzigingen.

Artikel 26. (Inwerkingtreding)

Artikel aangepast: de datum van inwerkingtreding is aangepast naar 1 januari 2026.

Artikel 27. (Citeertitel)

Artikel aangepast: 2021 is aangepast naar 2026.