STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 62488
22 december 2020

# Besluit van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 18 december 2020, nr. 2020-0000730468, tot vaststelling van een kader houdende de organisatie-inrichting van het CIO-stelsel binnen de Rijksdienst (Besluit CIO-stelsel Rijksdienst 2021)

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, tweede lid, van het Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst;

Besluit:

## *§ 1 Algemeen*

### Artikel 1 Definities

In dit besluit wordt verstaan onder:
a. *beveiligingsautoriteit:* een beveiligingsautoriteit, bedoeld in artikel 3 van het Besluit BVA-stelsel Rijksdienst 2021;
b. *beveiligingsautoriteit Rijk:* de beveiligingsautoriteit Rijk, bedoeld in artikel 7 van het Besluit BVA-stelsel Rijksdienst 2021;
c. *CIO:* een Chief Information Officer, bedoeld in artikel 3, eerste lid, en artikel 9, eerste lid;
d. *CIO Rijk:* de Chief Information Officer Rijk, bedoeld in artikel 10, eerste lid;
e. *CISO:* een Chief Information Security Officer, bedoeld in artikel 5, eerste lid, en artikel 9, derde lid;
f. *CISO Rijk:* de Chief Information Security Officer Rijk, bedoeld in artikel 10, eerste lid;
g. *Coördinatiebesluit:* Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst 2011;
h. *digitalisering:* het 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;
i. *grote ICT-component:* ICT-component vallend onder de definitie die in het Handboek portfoliomanagement Rijk wordt gegeven aan grote ICT-component;
j. *ICT:* Informatie- en communicatietechnologie;
k. *informatiebeveiliging:* het 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;
l. *informatiesysteem:* een samenhangend geheel van gegevensverzamelingen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie;
m. *informatievoorziening:* het geheel van mensen, middelen, informatiesystemen en maatregelen, gericht op de informatiebehoefte van een organisatie;
n. *portfoliomanagement:* proces van inventarisatie, registratie en actualisatie van wijzigingen in informatiesystemen, vastgelegd in een portfolio.

### Artikel 2 Reikwijdte

Dit besluit geldt voor de rijksdienst, zijnde de kerndepartementen en de daaronder ressorterende dienstonderdelen.

## *§ 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 11;
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 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; en
k. het aanmelden van activiteiten bij het Adviescollege ICT-toetsing, als bedoeld in artikel 4, eerste lid, van het Instellingsbesluit Adviescollege ICT-toetsing.

**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 2013 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 13, onder a, c en j, en de rijksbrede I-strategie, bedoeld in artikel 11, 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 13, 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; en
l. 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 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 2013, 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.

*§ 3. CIO Rijk en CISO Rijk*

**Artikel 10 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 11 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 en van een meerjarige I-strategie en -beleid voor de rijksdienst;
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.

**Artikel 12 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. De CIO Rijk voert namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties het overleg, bedoeld in artikel 3a van het Coördinatiebesluit.

**Artikel 13 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 11, onder d;
c. Het ontwikkelen en coördineren van het onderdeel informatiebeveiliging in de meerjarige I-strategie, bedoeld in artikel 11, 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; en
j. het coördineren van de aanpak van rijksbrede informatiebeveiligingsincidenten en -calamiteiten.

**Artikel 14 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; en
   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 departementen 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. CIO-Beraad en Rijks ICT-dashboard*

**Artikel 15 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 I-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 handvest CIO-beraad vast waarin de voorwaarden voor deelname en wijze van vergaderen nader zijn uitgewerkt. Dit handvest wordt minimaal tweejaarlijks geactualiseerd.

5. Het CIO-beraad heeft de volgende voorportalen:
   a) De CISO-raad;
   b) De Chief Technology Officer-raad, de CTO-raad;
   c) Het Tactisch Overleg Rijksnetwerken, TORN; en
   d) Het Tactisch Overleg Rijksbrede Voorzieningen, TORV.

6. De CISO-raad functioneert als voorportaal van het CIO-beraad op het gebied van informatiebeveiligingsbeleid. De CISO-raad wordt voorgezeten door CISO Rijk. Aan de CISO-raad nemen ten minste de departementale CISO's als lid deel.

7. De CTO-raad functioneert als voorportaal van het CIO-beraad op het gebied van ICT-aanbodsturing en informatietechnologie. De CTO-raad wordt voorgezeten door de CIO Rijk. Aan de CTO-raad nemen ten minste de directeuren van de ICT-dienstverleners binnen de rijksdienst als lid deel.

8. Het TORN functioneert als voorportaal van het CIO-beraad voor ontwikkeling, implementatie en beheer van de Rijksnetwerken. Het TORN wordt voorgezeten door een afgevaardigde van de CIO Rijk. Aan het TORN nemen ten minste afgevaardigden van de ICT-dienstverleners binnen de rijksdienst en afgevaardigden van de departementale CIO-offices deel.

9. Het TORV functioneert als voorportaal van het CIO-beraad op het gebied van Rijksbrede ICT-voorzieningen. Het TORV wordt voorgezeten door een afgevaardigde van de CIO Rijk. Aan het TORV nemen ten minste afgevaardigden van de departementale CIO-offices deel.

**Artikel 16 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 actualiseren van het Rijks ICT-dashboard en de kwaliteit van de gegevens van zijn ministerie.

*§ 5. Slotbepalingen*

**Artikel 17 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 18 Evaluatie**

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

**Artikel 19 Inwerkingtreding**

Dit besluit treedt in werking met ingang van 1 januari 2021.

**Artikel 20 Citeertitel**

Dit besluit wordt aangehaald als: Besluit CIO-stelsel Rijksdienst 2021.

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

*De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,*
*R.W. Knops*

## TOELICHTING

### Algemeen deel

#### *Ambitie*

De rijksdienst is continu in ontwikkeling om veilig, snel en betrouwbaar diensten te kunnen aanbieden aan de samenleving. Zij doet dat niet alleen. Het is de maatschappij die de overheid de digitale kansen biedt en innovatie stimuleert. Digitale ontwikkelingen als "Internet of Things", artificiële intelligentie en "Cloud Computing" zorgen voor veranderende behoeftes in de samenleving. Dergelijke digitale ontwikkelingen dagen de rijksdienst uit om zelf ook volgende stappen te zetten in het digitale domein en zo toegevoegde waarde te blijven creëren in een steeds sneller digitaliserende wereld. De Chief Information Officers (CIO's) binnen de Rijksdienst vervullen hier een sleutelrol in. Als de digitale leiders in het CIO-stelsel werken zij niet alleen samen aan de oplossingen van vandaag, maar geven zij richting aan een digitale transitie voor de ontwikkelingen van morgen.

Het is het digitaal leiderschap van de CIO's dat binnen een goed ingericht CIO-stelsel een zo maximaal mogelijke maatschappelijke opbrengst beoogt te creëren. Dit besluit vormt een basis om tijdig en succesvol de beleids- en bedrijfsvoeringdoelstellingen met behulp van ICT en informatiesystemen in de rijksdienst te kunnen realiseren. Hierbij moet ook altijd oog zijn voor de risico's van digitalisering, waarmee een goede verhouding en samenwerking tussen de CIO's en Chief Information Security Officers (CISO) een randvoorwaarde is voor succes. Deze beide functies, CIO en CISO, staan centraal in dit besluit.

In dit besluit is met het digitaal leiderschap bedoeld dat de CIO de digitale en technologische ontwikkelingen voortdurend volgt en daarop een strategische visie voorbereidt. Welke digitale keuzes maakt de organisatie en hoe worden ze geïmplementeerd? Dit besluit stelt de verantwoordelijk bewindspersoon daarmee in staat om ontwikkelingen als toenemende beveiligingsrisico's en het toenemende dataverkeer tijdig en strategisch af te wegen en daarin te kiezen. De CIO stimuleert vervolgens hiervoor het (technologische) innovatieproces in het ministerie. Het tijdig anticiperen dat dit besluit beoogt, leidt dan meer tot stapsgewijze vernieuwing van informatiesystemen en minder tot nieuwe, grote ICT-projecten. Dat continue, stapsgewijze innovatieproces heet de digitale transformatie. Deze innovatie binnen een organisatie is gebaseerd op een digitale of technologische ontwikkeling en is daarmee een technologische gedreven innovatie. De rol van de CIO laat zich dan ook het beste samenvatten als de digitale leider die de informatievoorziening richting geeft bij het realiseren van dat deel van de maatschappelijke opgave waarbij digitalisering een oplossing zou kunnen zijn. Hij of zij is daarin de partner van de beleidskolom en het uitvoeringsveld van het ministerie.

Daarnaast helpt het dat alle CIO's en Chief Information Security Officer's (CISO's) groeien naar een vergelijkbaar takenpakket en vergelijkbare bevoegdheden krijgen, ook al wordt rekening gehouden met de verschillen in de organisaties. Elke digitale leider is namelijk afhankelijk van de verantwoordelijke voor beleid of de eigenaar van een (informatie)proces. Met een vergelijkbare invloed voor alle CIO's om strategisch keuzes in de organisatie te kunnen implementeren, ontstaat een digitaal verandervermogen van de rijksdienst als geheel. De vergelijkbaarheid van de CIO's schept namelijk het vertrouwen dat samen voortdurend digitaal transformeren met alle organisaties in de rijksdienst mogelijk is.

De formalisering van het CIO-stelsel dat in dit besluit wordt nagestreefd dient nog een ander doel: het faciliteert het lerend vermogen binnen het stelsel. Samenwerking vormt de basis voor een cultuur van kennisdeling, anticiperen en reflecteren binnen het CIO-stelsel. Door vergelijkbare taken per functionaris en georganiseerde samenwerkingsverbanden ontstaat het vermogen om van elkaar te leren. Hoe ontwikkelt de crisisstructuur in het CIO-stelsel bij informatiebeveiligingsincidenten zich het beste? Hoe houdt digitalisering Nederland droog en hoe zorgt de juiste software dat de bevolking langer vitaal blijft en we steeds meer ziektes vroegtijdig kunnen behandelen? Het CIO-stelsel faciliteert het delen van kennis en ervaring met elkaar, onder andere in het CIO-beraad en de CISO-raad.

#### *Aanleiding*

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.[1] Dit besluit is een invulling daarvan. In dit besluit zijn naast de taken en bevoegdheden van CIO binnen de rijksdienst ook die van de CIO Rijk, de CISO Rijk en de CISO's

[1] *Kamerstukken II* 2019/20, 26 643, nr. 656, p. 3.

binnen de rijksdienst vastgelegd. Voorts omvat dit besluit de positie van het CIO-beraad en zijn voorportalen, zoals de CISO-raad. Hiermee wordt de aanbeveling uit het onderliggende ADBTOPConsult-rapport opgevolgd om de rol van de departementale CIO verder te versterken en te verhelderen; zij het dan niet beperkt tot een taakbesluit gericht op de CIO-functie alleen, maar in dit besluit dat alle voornoemde rollen en hun onderlinge samenhang binnen het CIO-stelsel omvat.[2]

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.[3] Binnen het CIO-stelsel is sindsdien het besluitvormingsproces over ICT en de digitale publieke dienstverlening binnen de rijksdienst ontwikkeld. De rijksbrede kaders die voor het stelsel zijn ontwikkeld, zijn veelal gericht op het object van sturing en verantwoording, zoals de informatiesystemen, de informatievoorziening en digitalisering in den brede, en in veel mindere mate op de functies binnen het stelsel zelf. Belangrijke ontwikkelingen, gericht op die functies, zijn: de opkomst van CIO's in de uitvoering bij dienstonderdelen; de verschuivende rol van CIO's van toetsend achterin de keten naar adviserend en digitaal leiderschap tonend aan de voorzijde en de creatie van de CISO-functie voor informatiebeveiliging. Dit besluit formaliseert deze ontwikkelingen, geeft richting en helderheid en versterkt daarmee het besturingsmodel en het besluitvormingsproces in het CIO-stelsel.

### *Uitgangspunten*

De grootte van de rijksdienst met veel verschillende organisaties enerzijds en de veelheid aan digitale ontwikkelingen in de maatschappij anderzijds, maakt dat een hechte samenwerking tussen de CIO's, CISO's en andere betrokkenen bij het CIO-stelsel een belangrijk uitgangspunt is in dit besluit. Een goede interdepartementale samenwerking vergroot de wendbaarheid waarmee de rijksoverheid kan anticiperen op een digitale ontwikkeling en kan reageren op een digitale dreiging. Het CIO-beraad en ook de CISO-raad, als adviesraad voor het CIO-beraad, spelen bij deze interdepartementale samenwerking een belangrijke rol. De CIO Rijk en onderscheidenlijk de CISO Rijk zijn de voorzitters van deze raden en coördineren deze samenwerking. Naast een goede samenwerking binnen de rijksdienst is ook in toenemende mate een actieve samenwerking met kennisinstituten en het bedrijfsleven van belang. Deze samenwerking zorgt ervoor dat onder andere de CIO's en de CISO's in het CIO-stelsel kunnen anticiperen op die digitale ontwikkelingen of dreigingen.

Zoals in de brief van 20 december 2019 is benoemd, is een ander uitgangspunt dat elke minister verantwoordelijk blijft voor de informatievoorziening in het eigen ministerie.[4] Dit geldt voor zowel de bedrijfsvoering als de digitalisering binnen de publieke taak van een ministerie - ook wel genoemd: het primaire proces. De effectiviteit van dit besluit is gebaat bij voldoende ruimte voor maatwerk en flexibiliteit, vanwege de veelheid aan organisaties en taakgebieden binnen de rijksdienst, maar ook de snelheid van digitale ontwikkelingen: de digitale transformatie. De noodzaak voor deze flexibiliteit is reeds in 2008, bij de start van het stelsel onderkend. De reden hiervoor was toen dat, door de strategische positionering van een CIO, elke minister in staat moest kunnen zijn om het informatiemanagement te organiseren dat aan alle professionele standaarden voldoet.[5] Daarnaast biedt dit besluit instrumenten waarmee de functionarissen in het CIO-stelsel voldoende armslag en flexibiliteit krijgen om effectief te zijn. In dit besluit is hierbij een algemene uitzonderingsclausule opgenomen waarmee, op onderdelen, beargumenteerd en na overleg met de Minister van Binnenlandse Zaken en Koninkrijksrelaties, kan worden afgeweken van dit besluit wanneer dit de effectiviteit van de met dit besluit beoogde doelen redelijkerwijs ten goede komt.

Tot slot is het lerend vermogen in het CIO-stelsel van de rijksdienst een belangrijk uitgangspunt. Het Adviescollege ICT-toetsing (Adviescollege) draagt als onafhankelijk adviescollege voor het CIO-stelsel bij aan dat lerend vermogen door het toetsen, adviseren en ook het delen van kennis. Om die reden sluit dit besluit goed aan bij het instellingsbesluit van het Adviescollege ICT-toetsing. Zo regelt dit besluit dat de CIO een eigen eerste oordeel over een groot ICT-project of -activiteit geeft voor aanvang, alvorens hij of zij bij het Adviescollege een verzoek indient voor advies.

### *Het CIO-stelsel Rijksdienst*

De CIO is de centrale functie binnen het CIO-stelsel. De primaire rol van de CIO is om ervoor te zorgen dat het ministerie waar hij of zij werkzaam is tijdig kunnen inspelen op ontwikkelingen op het gebied

---

2 *Overzicht opvolging van aanbevelingen uit het ABDTOPConsult-rapport "IV en overheid: de pubertijd voorbij."* bijlage bij *Kamerstukken II* 2019/20, 26 643, nr. 656, p. 2.
3 *Kamerstukken II* 2007/08, 26 643, nr. 128, p. 7.
4 *Kamerstukken II* 2019/20, 26 643, nr. 656, p. 3.
5 *Kamerstukken II* 2008/09, 26 643, nr. 135, p. 1-2.

van ICT en digitalisering. Hieruit vloeit de taak van de CIO voort om vanuit deze ontwikkelingen een vertaalslag te maken naar het zorgdragen voor de ontwikkeling en het beheer van de informatievoorziening en de informatiesystemen binnen het ministerie. Dit uit zich in taken van de CIO bij de ontwikkeling van het beleid, de uitvoering en ook de bedrijfsvoering in het ministerie, in afstemming met de verantwoordelijken voor het beleid of een taakveld, zoals een directeur-generaal. De CIO heeft daarbij de beschikking over een overzicht van informatiesystemen en ICT-projecten van het ministerie. Op basis daarvan is er een inzicht in de prioritering van ICT-activiteiten, het zogeheten portfolio. Op basis daarvan kan de CIO zijn of haar visie bepalen om op digitale ontwikkelingen in de samenleving in te spelen binnen zijn of haar ministerie. Het gaat in die visie onder meer over het onderhoud en beheer van bestaande informatiesystemen en ook hoe nieuwe ICT-projecten en -wijzigingen al in productie zijnde informatiesystemen en diensten vernieuwen, gebaseerd op een vorm van levenscyclusmanagement. Per organisatie binnen de rijksdienst verschilt het waar in de functie van de CIO de focus ligt. Soms ligt meer nadruk op het formuleren van beleid en advisering over de digitaliseringsaspecten. Bij andere CIO's ligt meer nadruk op beheersing, zoals het geven van CIO-oordelen en de kwaliteitsborging. Tot slot is er de CIO waar meer de nadruk ligt op de ICT-uitvoering. Denk hierbij aan de rol van het hoofd van een i-regieonderdeel binnen het departement of als feitelijk opdrachtgever van grote ICT-trajecten. In het besluit is er ruimte voor deze diversiteit, omdat daarmee het besluit aansluit op de specifieke opgaven van een organisatie.

Als een van de taken van de CIO betrekking heeft op een digitale dreiging dan helpt de risicoanalyse van de CISO binnen het CIO-office om de departementale CIO zijn of haar taken te laten uitvoeren. De CIO moet kunnen adviseren en oordelen over alle aspecten van digitalisering en informatievoorziening, waaronder aspecten zoals informatiebeveiliging, privacy en de ontwikkeling en het beheer van informatiesystemen, in elk stadium van het uitvoeringsproces, de beleidsontwikkeling of het bedrijfsvoeringproces. Nieuwe projecten en wijzigingen in al in productie zijnde informatiesystemen met een grote ICT-component, kunnen in principe pas starten ná een positief CIO-oordeel.

Informatievoorziening en digitalisering kennen vele aspecten. Afhankelijk van de specifieke behoefte binnen een ministerie en het stelsel als geheel kunnen aan die aspecten verschillend gewicht worden gegeven. Aan de hand van die behoeften kan per aspect worden bepaald hoe er wordt gestuurd en hoe ervoor de ontwikkeling en het beheer van informatiesystemen wordt zorggedragen. In dit besluit is weloverwogen gekozen om het aspect informatiebeveiliging een centrale plek te geven en de taken en bevoegdheden van de CISO's en CISO Rijk hiervoor te expliciteren. Dit wil nadrukkelijk niet zeggen dat andere aspecten en functies minder relevant zijn, maar wel dat een heldere taakinvulling juist voor informatiebeveiliging op alle niveaus van essentieel belang is. Een heldere taakinvulling in het stelsel maakt namelijk inzichtelijk hoe er wordt gestuurd en zorggedragen voor de ontwikkeling en het beheer van de informatiesystemen.

De primaire functie van het CIO-beraad en de CISO-raad als voorportaal voor het CIO-beraad, is een sterke interdepartementale samenwerking tussen CIO's, als het gaat om het anticiperen op digitale en procesmatige ontwikkelingen, respectievelijk de CISO's, als het gaat om het reageren op digitale dreigingen. Het CIO-beraad heeft een meerjarige strategische visie op de ontwikkeling van de informatievoorziening in de rijksdienst; de meerjarige visie van de CISO-raad over informatiebeveiliging is hiervan een onderdeel. Beide visies beslaan beleidsontwikkeling, de uitvoering van beleid en de bedrijfsvoering. Indien nodig geven rijksbrede richtlijnen of kaders van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, vastgesteld na overleg met de ministers die het aangaat, aan hoe op deze digitale ontwikkelingen uit die meerjarige visie door de rijksdienst moet worden gereageerd.

### *Reikwijdte van dit besluit*

Op basis van het Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst (Coördinatiebesluit) heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties een aantal verantwoordelijkheden met betrekking tot informatiesystemen binnen de rijksdienst. De Minister van Binnenlandse Zaken en Koninkrijksrelaties kan, na overleg met de andere ministers, kaders vaststellen; gegevens over informatiesystemen bij andere ministeries opvragen en er moet met hem of haar op grond van artikel 3, onderdeel a, van het Coördinatiebesluit worden overlegd alvorens een minister een CIO aanstelt of ontslaat. Binnen de reikwijdte van het Coördinatiebesluit worden die verantwoordelijkheden in dit besluit verder uitgewerkt. De reikwijdte van het Coördinatiebesluit is dat bepalingen betrekking kunnen hebben op een ministerie of een organisatieonderdeel van een der ministeries. Zelfstandige bestuursorganen en Hoge Colleges van Staat maken geen onderdeel uit van de rijksdienst. Het besluit is daarom niet dwingend van toepassing op deze organisaties, maar kan voor hen wel richtinggevend zijn. Bij de hiervoor genoemde coördinerende verantwoordelijkheden van de Minister van Binnenlandse Zaken en Koninkrijksrelaties hoort een verantwoordingsplicht en informatievoorziening richting de Tweede Kamer.

### *Toepasselijkheid van dit besluit op departementale CIO-stelsels*

De vorming van een departementale visie - ook wel: meerjarig informatieplan - en de implementatie van rijksbrede kaders en nieuw informatievoorzienings- en ICT-beleid in het ministerie is de verantwoordelijkheid van de departementale CIO. Daarvoor is hij of zij belast met het inrichten van een CIO-stelsel in het ministerie. Door middel van dit stelsel kan hij of zij informatie opvragen over de status van de implementatie van nieuw beleid of rijksbrede kaders en heeft hij of zij een portfolio van de informatiesystemen en -diensten, grote ICT-projecten en grote wijzigingen in al in productie zijnde informatiesystemen en diensten. Binnen een departementaal stelsel kan een CIO daarbij verschillende rollen hebben. Hij of zij heeft bijvoorbeeld de rol van opdrachtgever of eigenaar van een informatiesysteem of informatieproces. Ook kan hij of zij de rol van kwaliteitsborger hebben, juist onafhankelijk van een opdrachtgever of eigenaar. Samenhang en evenwicht tussen die rollen vormt een waarborg voor realistische ambities, betere besluiten over haalbaarheid en veiligheid en meer succesvolle uitkomsten van ICT-uitvoeringsactiviteiten. Voor het kunnen dragen van deze taken beschikt de CIO over een CIO-office, waarvan de departementale CISO een onderdeel is. De CIO heeft in zijn of haar office de beschikking over voldoende kennis en ervaring op de beleidsterreinen, ICT-architectuur en de bedrijfsvoering in het ministerie. Deze kennis en ervaring in het CIO-office is noodzakelijk, omdat door de digitale ontwikkelingen in de maatschappij steeds vaker en meer ICT wordt toegepast binnen de verschillende beleidsterreinen en de bedrijfsvoering. De kennis en ervaring stelt een CIO-office in staat digitaliseringsvraagstukken en -beleid integraal te benaderen en daarmee het juiste evenwicht te vinden tussen beleidsdoelen enerzijds en onder meer informatievoorzieningsaspecten als informatiebeveiliging, privacy, openbaarheid en duurzame toegankelijkheid anderzijds. Voorgaande taken verricht een CIO-office in afstemming met de verantwoordelijken voor de taakvelden of het beleid, zoals de desbetreffende directeur-generaal.

## Artikelsgewijze toelichting

### *Artikel 1 (Definities)*

Dit artikel definieert enkele veelgebruikte bepalingen in dit besluit.

De definitie van informatievoorziening in dit artikel maakt duidelijk dat informatievoorziening een begrip is dat veel aspecten omvat ten aanzien van het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van die organisatie. Het betreft hier onder meer de aspecten ontwikkeling en beheer van informatiesystemen, informatiebeveiliging, architectuur, gegevens, gegevensverzamelingen, privacy en informatiehuishouding.

De definitie van portfoliomanagement in dit artikel beschrijft het proces van inventarisatie, registratie en actualisatie van wijzigingen in informatiesystemen in een ministerie. Het doel van dit proces is om op basis van het overzicht deze wijzigingen te kunnen prioriteren aan de hand van de beschikbare middelen en de wensen om die middelen in te zetten. Het Handboek Portfoliomanagement Rijk vult dit proces verder in.

### *Artikel 2 (Reikwijdte)*

In dit artikel wordt bepaald op welke organisaties in de rijksoverheid dit besluit van toepassing is. Het betreffen alle kerndepartementen en de daaronder ressorterende dienstonderdelen. Het besluit is niet van toepassing op zelfstandige bestuursorganen.

### *Artikel 3 (CIO-functie)*

In het eerste lid staat beschreven dat de CIO ressorteert onder de secretaris-generaal van het ministerie. De reden hiervoor is dat ICT allang niet meer beperkt is tot bedrijfsvoering, ICT is vaak een kernaspect van het beleid. Het is daarom belangrijk dat de CIO op het hoogste niveau van het ministerie is geborgd. De integraliteit van de coördinatie, sturing en advisering over de digitalisering en informatievoorziening is hiermee gediend.

Elk ministerie zal haar eigen inspanning moeten leveren en aanpassing moeten doen om hieraan tegemoet te kunnen komen. De positionering van de CIO onder de secretaris-generaal moet gezien worden als een groeimodel en het kan niet verwacht worden dat na de inwerkingtreding van dit besluit elk ministerie hier gelijk aan voldoet. Een uitzondering hierop is daarom mogelijk op grond van artikel 17 van dit besluit.

Het tweede lid beschrijft de taak van de departementale CIO als digitaal leider. De CIO kent de digitale trends en beoordeelt ze op relevantie voor zijn of haar organisatie. In een meerjarig departementaal

informatieplan formuleert de departementale CIO de strategische visie op digitale transformatie met prioritaire informatiebeleidsdoelstellingen op basis van de relevante digitale trends voor het ministerie. De departementale CIO wordt daarbij gestuurd door het departementale beleid en de departementale uitvoering enerzijds en het interdepartementale informatiebeleid anderzijds. Hij of zij formuleert de strategische visie op digitale transformatie en de prioritaire doelstellingen in overleg met het lijnmanagement van die informatiesystemen in de bedrijfsvoering of het primaire proces (de beleidsterreinen of taakvelden), omdat die informatiesystemen en beoogde wijzigingen daar een onlosmakelijk onderdeel van vormen. Het lijnmanagement is uiteindelijk ook integraal verantwoordelijk voor de realisatie van de beleids- en uitvoeringsdoelstellingen, die met deze digitalisering en informatievoorziening wordt beoogd. De CIO van een departement is belast met de inrichting van het CIO-stelsel binnen het betreffende ministerie. Hij of zij is belast met de taak om een departementaal stelsel in te richten en voor welk van die organisaties dus een eigen CIO en CISO gewenst zou zijn. De departementale CIO kan vervolgens taken en bevoegdheden uit dit besluit aan hen mandateren.

De digitalisering binnen de publieke taak van ministeries neemt toe. De CIO neemt daarom deel aan de bestuursraad, of een daarmee vergelijkbaar overlegorgaan in een ministerie, omdat zijn of haar strategische visie ten aanzien van het anticiperen en implementeren van digitale ontwikkelingen - de digitale transformatie - de verschillende uitvoerings- en beleidsdoelen van een ministerie kunnen raken. De departementale CIO is daarmee de digitale leider die de informatievoorziening richting geeft bij het realiseren van dat deel van de maatschappelijke opgave waarbij digitalisering een oplossing zou kunnen zijn. Van deze bepaling in het vierde lid van dit artikel kan beargumenteerd worden afgeweken (op grond van artikel 17 van dit besluit).

Het vierde en vijfde lid regelt dat er een CIO-office is en welke kennis en expertise nodig is om de digitale transformatie tot een succes te maken en uitvoering te geven aan bestaand beleid. De samenstelling van het CIO-office is een departementale aangelegenheid, maar zal zo moeten worden ingericht dat het over voldoende kennis, ervaring en capaciteit beschikt om aan de taken van de CIO, zoals verwoord in het vierde artikel, te voldoen.

***Artikel 4 (Taken departementale CIO)***

In dit artikel staan de taken benoemd van de departementale CIO van een ministerie. Het betreft hier geen uitputtende lijst van taken die de minister, die belast is met de leiding van een ministerie, opdraagt aan de departementale CIO. De departementale CIO kan deze taken mandateren aan andere CIO's binnen het CIO-stelsel dat is ingericht in het ministerie. CIO's van dienstonderdelen zijn daarbij uiteraard gehouden aan het bepaalde in artikel 5, vierde lid van dit besluit en verstrekken de departementale CIO gevraagd en ongevraagd de informatie die noodzakelijk is voor de uitoefening van diens taken voor het departementale stelsel.

Nu de informatievoorziening en de digitalisering een groot onderdeel vormt van de bedrijfsvoering en het primaire proces in een departement is het belangrijk dat de departementale CIO regelmatig, onder meer door middel van het portfolio, het lijnmanagement en de minister van het ministerie adviseert. Hij of zij zorgt ervoor dat de bestuursraad informatiebeleid formuleert en hij of zij adviseert over de gevolgen van (voorgenomen) wet- en regelgeving. Daarbij gebruikt hij of zij het meerjarige departementale informatieplan. Het meerjarig informatieplan beschrijft de strategische visie met prioritaire informatiebeleidsdoelstellingen op digitale transformatie binnen het primair proces. Deze doelstellingen kunnen om verschillende redenen prioritair zijn, bijvoorbeeld vanwege politieke urgentie, ambitie of impact binnen het departementale informatiebeleid. De prioritaire doelstellingen zijn een vertaling van de visie, strategie en beleidsdoelstellingen van het departement enerzijds en de beleidsprioriteiten uit de meerjarige I-strategie van de CIO Rijk anderzijds. Het meerjarige informatieplan kent een drieledig doel: het versterkt intern overzicht en inzicht in de prioriteiten, het stimuleert een cultuur van kennisdeling en het is een voorwaarde voor goede verantwoording aan de Tweede kamer. In een kader worden de aspecten van het meerjarig departementaal informatieplan verder uitgewerkt.

Niet alleen grote ICT-projecten, maar ook grote wijzigingen in bestaande informatiesystemen en informatieprocessen passen binnen de strategische visie van de departementale CIO en de digitale transformatie die hij of zij voorstaat. Het is de taak van de departementale CIO om te bewerkstelligen dat de verantwoordelijken binnen een beleidsterrein of taakveld de technologisch gedreven innovaties implementeren in overeenstemming met de strategische visie die de CIO in het ministerie heeft opgesteld en door de minister is vastgesteld. Hij of zij stimuleert echter niet alleen de digitale transformatie, maar bewaakt door middel van het portfolio ook de kwaliteit van bestaande informatiesystemen en stimuleert ICT-activiteiten gericht op de continuïteit van deze systemen indien noodzakelijk. De CIO heeft hier in het departement de rol van een digitaal leider. Hij of zij is niet alleen actief betrokken bij de digitale transformatie waarin technologische gedreven innovaties op de juiste wijze door verantwoordelijken in een taakveld of beleidsterrein worden geïmplementeerd, maar bevordert ook het lerend vermogen op het gebied van digitalisering en informatievoorziening in het ministerie,

onder andere door kennisdeling. Het is zijn of haar taak om in een cultuur te investeren die dit mogelijk maakt. Daarbij moet in het bijzonder gedacht worden aan het investering in een actieve samenwerking met kennisinstituten en het bedrijfsleven. De kennis en de kansen om adequaat te anticiperen op die digitale ontwikkelingen of dreigingen worden daar in veel gevallen gecreëerd. Dat biedt mogelijkheden voor de CIO's en de CISO's in het stelsel en het is de taak van de departementale CIO om die kennis en kansen maximaal te benutten voor de eigen organisatie en het lijnmanagement en de relevante actoren in het CIO-stelsel daarvan te overtuigen. Interdepartementale overleggen, zoals het CIO-beraad, kunnen vervolgens de plek zijn om deze opgedane kennis en inzichten ook buiten de organisatie, maar binnen de rijksdienst, te delen.

De departementale CIO heeft verder de taak om, gegeven zijn of haar eigen departementale informatieplan, informatiesystemen, informatievoorzieningsbeleid, digitaliseringsbeleid te ontwikkelen en te coördineren voor de organisatie. Tevens is het de taak van de departementale CIO om de informatiesystemen te beheren op grond van dit beleid. De digitale trends die elkaar snel opvolgen maken dat het belang van een goede strategische visie op de digitale transformatie ten aanzien van wet- en regelgeving en beleids- en uitvoeringstraject binnen een ministerie groeit. Hij of zij neemt daarbij de beschikbare rijksbrede ICT-voorzieningen in acht vanuit het principe te streven naar uniformiteit, zoals dit onder meer is voorgeschreven in richtlijnen zoals de Nederlandse Overheid Referentie Architectuur. De CIO kan, passend binnen informatievoorzieningsbeleid en digitaliseringsbeleid geldend voor de hele rijksdienst, beleid ontwikkelen en kaders en richtlijnen opstellen, indien dat nodig is voor de continuïteit van informatiesystemen of de digitale transformatie binnen het ministerie. Het beleid of de kaders en richtlijnen sluiten dan aan bij de strategische visie op de digitale transformatie van het ministerie, zoals hij of zij dat verwoordt in het meerjarige departementale informatieplan. Het meerjarige informatieplan bevat een financiële paragraaf waarin de ICT-activiteiten, zoals de CIO die voorziet, beargumenteerd van een financieel gevolg worden voorzien. Daarnaast zijn er kaders en richtlijnen die gelden voor alle ministeries, bijvoorbeeld ter bevordering van de eenheid, kwaliteit, informatiebeveiliging daaronder begrepen, en efficiëntie van informatiesystemen, zoals bedoeld in het Coördinatiebesluit. De CIO, als digitaal leider van een organisatie, stimuleert dat de verantwoordelijken in een taakveld of op een beleidsterrein deze voorzieningen, kaders en richtlijnen goed gebruiken en implementeren. De CIO voert vervolgens dus zijn of haar meerjarige departementale informatieplan uit. Het is aan de departementale CIO om het verantwoordelijk lijnmanagement van het ministerie en de CIO Rijk te informeren en te adviseren over het gebruik van deze voorzieningen, kaders en richtlijnen.

Bij goed beheer van een ICT-infrastructuur binnen het ministerie hoort een goed integraal portfolio- en levenscyclusmanagement van informatiesystemen en informatieprocessen, zodat de samenhang tussen ICT-(door)ontwikkeling en ICT-beheer bewaakt wordt. De CIO is, in samenspraak met de CISO, belast met de continue vernieuwing van informatiesystemen op het gebied van informatiebeveiliging, privacy en de technologische ontwikkeling van functionaliteiten. Elke CIO beheert voor zijn of haar eigen organisatie daartoe een portfolio waar, op basis van een overzicht van de informatiesystemen en informatieprocessen, een inzicht kan worden gegeven over de prioriteiten binnen het levenscyclusmanagement. De CIO streeft hier naar integraal portfoliomanagement waarbij zowel nieuwe projecten en wijzigingen binnen al in productie zijnde informatiesystemen en informatieprocessen worden geprioriteerd en gewogen tegen prioriteiten in beheer en onderhoud. Door daarbij diensten als aggregatieniveau te gebruiken in het portfolio kan de levenscyclus van een informatiesysteem inzichtelijk worden gemaakt vanuit het perspectief van de eindgebruiker. Onder een (digitale) dienst wordt daarbij verstaan: samenhangende dienstverlening, uitgevoerd met informatiesystemen, vanuit samenhangende beleidsdoelstellingen en gericht op specifieke doelgroepen en daarmee samenhangende procesvelden en (maatschappelijke) baten. De CIO bespreekt de levenscyclus van deze diensten en informatiesystemen regelmatig met het verantwoordelijk lijnmanagement binnen een taakveld of beleidsterrein, zoals een directeur-generaal. De departementale CIO bespreekt het levenscyclusmanagement van verschillende informatiesystemen en informatieprocessen in alle portfolio's binnen het ministerie in samenhang in de bestuursraad.

Tot slot is een departementale CIO belast met de taak om de beheersbaarheid, de slaagkans en de risico's te beoordelen van voorgenomen nieuwe projecten en van wijzigingen binnen in productie zijnde informatiesystemen en diensten met een grote ICT-component gericht op de wijziging, continuïteit of vernieuwing van informatiesystemen. Het CIO-oordeel dient als een kwaliteitsinstrument en vergroot het vermogen binnen de organisatie om te leren hoe de beheersbaarheid en slaagkans kan worden vergroot, terwijl de risico's worden verkleind. Bij dit oordeel maakt de CIO gebruik van het kwaliteitskader CIO-oordelen Rijksoverheid. Het lerend vermogen binnen het CIO-stelsel wordt voorts verder vergroot met het externe kwaliteitsinstrument van het advies van het Adviescollege ICT-toetsing. Zoals bedoeld in het Instellingsbesluit Adviescollege ICT-toetsing meldt de CIO activiteiten aan bij het college namens de minister. Vanwege de coördinerende taken van de CIO Rijk informeert de CIO de CIO Rijk gevraagd en ongevraagd over de informatie, zoals in artikel 6, eerste lid, van het Coördinatiebesluit is bedoeld voor zover naar dit redelijkerwijs noodzakelijk is voor

de uitoefening van diens taken. Het betreft hier onder meer de CIO-oordelen en de bestuurlijke reacties op adviezen van het Adviescollege ICT-toetsing. Geleerde lessen uit deze oordelen en reacties kunnen het stelsel versterken en indien nodig door de CIO Rijk worden besproken in het CIO-beraad. Het gaat daarnaast bijvoorbeeld om het uitvragen van inlichtingen over de levenscyclus of de informatiebeveiliging van een bepaald informatiesysteem of het geheel van informatiesystemen in de vorm van een portfolio, zoals bedoeld in artikel 11, onderdeel h. Het gaat hier ook om informatie en gegevens over de wijze waarop de kaders door de ministeries worden nageleefd. Als de CIO Rijk constateert dat de gestelde kaders niet worden nageleefd, dan informeert hij of zij hier de Minister van Binnenlandse Zaken en Koninkrijksrelaties over. De informatie die de CIO Rijk aan de departementale CIO's uitvraagt en die de departementale CIO's aan de CIO Rijk verstrekken wordt bepaald en geregeld in het Informatiestatuut, dat geldt voor de rijksdienst. De CIO's verstrekken de CIO Rijk enkel de informatie die redelijkerwijs gevraagd kan worden en benodigd is voor diens taakuitoefening.

***Artikel 5 (Bevoegdheden departementale CIO)***

Het eerste lid beschrijft de mogelijkheid van de departementale CIO om, na overleg met de secretaris-generaal, de minister rechtstreeks te informeren als zijn of haar taakuitoefening, zoals uiteengezet in het vorige artikel, hiertoe aanleiding geeft. Het rechtstreeks informeren houdt in dat de departementale CIO zonder tussenkomst van de ambtelijke leiding of andere dienstonderdelen van het ministerie de minister kan informeren, indien zijn of haar taken hiertoe aanleiding geven. Deze mogelijkheid wordt toegepast, nadat overleg met de secretaris-generaal van het ministerie heeft plaatsgevonden. In de praktijk is deze mogelijkheid dan ook een ultimum remedium. Ingeval een ministerie door meer dan één bewindspersoon wordt geleid, kan de departementale CIO zowel de minister die belast is met de leiding van het ministerie als de minister zonder portefeuille of de staatssecretaris rechtstreeks informeren.

Het tweede lid beoogt de volwassenheid van het CIO-stelsel tot uitdrukking te brengen, omdat het de CIO de mogelijkheid geeft om ten aanzien van activiteiten met een grote meerjarige ICT-component kwaliteitstoetsen uit te voeren. Hij of zij kan ook een opdracht tot een externe kwaliteitstoets geven. Het betreffen hier audits en rapportages die inzicht geven in de kwaliteit van al dan niet voorgenomen activiteiten gericht op de wijziging, continuïteit of vernieuwing van informatiesystemen. Het gaat hier om eigen adviezen of externe kwaliteitstoetsen, bijvoorbeeld een Gatewayreview, rapportage van de Auditdienst Rijk of een gecontracteerde partij van buiten de rijksoverheid.

In het derde lid staan de gevolgen van een negatief CIO-oordeel beschreven. Wijzigingen met een grote ICT-component kunnen niet starten zonder een positief CIO-oordeel. De risico's zijn vanwege de vaak (geldelijke) omvang van deze activiteiten groot en rechtvaardigen daarmee ook de positie van deze interne kwaliteitstoets van het CIO-oordeel. Voorts stelt het CIO-oordeel de minister in staat voorgenomen activiteiten met een grote ICT-component intern te toetsen alvorens hij of zij aan zijn of haar verplichting voldoet het Adviescollege ICT-toetsing te verzoeken om een advies over de risico's en slaagkans van het ICT-project. Een negatief CIO-oordeel wordt geagendeerd in de bestuursraad. De secretaris-generaal en ook de minister die het aangaat kunnen beiden beargumenteerd afwijken van het gegeven CIO-oordeel.

Naast het rechtstreeks informeren van de bewindspersonen is het ook van belang dat de departementale CIO rechtstreeks informatie kan uitvragen over aangelegenheden die voor de uitoefening van zijn taken nodig is. Het vierde lid strekt hiertoe. Het gaat bijvoorbeeld om het uitvragen van inlichtingen over de levenscyclus of de informatiebeveiliging van een bepaald informatiesysteem of het geheel van informatiesystemen in de vorm van een portfolio, zoals bedoeld in artikel 4, onderdeel g.

***Artikel 6 (Departementale CISO)***

In het eerste lid staat beschreven dat de CISO rechtstreeks ressorteert onder de CIO van het ministerie.

Het tweede lid beschrijft de verantwoordelijkheid van de CISO. De CISO kent de actuele dreigingen voor de informatiesystemen in het ministerie en is op de hoogte van de mate van informatiebeveiliging daarvan. Hij of zij formuleert en ontwikkelt op basis hiervan het informatiebeveiligingsbeleid binnen het ministerie en coördineert de naleving ervan. Voor dat laatste ondersteunt hij of zij het verantwoordelijk lijnmanagement van het ministerie bij de implementatie en naleving. De CISO ondersteunt daarmee de strategische visie op de digitale transformatie van de CIO onder wie hij of zij ressorteert.

***Artikel 7 (Taken departementale CISO)***

In dit artikel staan de taken benoemd voor de departementale CISO. De departementale CISO kan deze taken mandateren aan CISO's binnen het CIO-stelsel dat in een ministerie is ingericht. Digitale

dreigingen verdienen in een volwassen CIO-stelsel continu de aandacht. Risicoanalyses, informatiebeveiligingsadviezen en het toezien op de naleving van informatiebeveiligingskaders moeten de CIO in staat stellen de digitale transformatie in het ministerie verantwoord tot een succes te brengen.

Nu de informatiebeveiliging een belangrijk onderdeel vormt van de bedrijfsvoering of het primaire proces, vanwege continue digitale dreigingen in overheidsorganisaties, is het belangrijk dat de CISO regelmatig, onder meer door middel van het portfolio informatiebeveiliging, de departementale CIO en het verantwoordelijk lijnmanagement van het ministerie adviseert. Hij of zij adviseert hen over informatiebeveiligingsbeleid en over het risicomanagement van informatiebeveiliging van (voorgenomen) wet- en regelgeving, daarbij gebruikt hij of zij indien nodig het departementale informatieplan waarin de strategische visie van de CISO op informatiebeveiliging is opgenomen.

Het is de taak van de CISO om te bewerkstelligen dat het lijnmanagement binnen een beleidsterrein of taakveld zich bewust is van digitale dreigingen en de risico's van informatiebeveiliging en dat dit bewustzijn wordt vergroot. De CISO houdt in de gaten dat de organisatie de juiste informatiebeveiligingsmaatregelen neemt en implementeert, bijvoorbeeld op basis van de Baseline Informatiebeveiliging Overheid. De CISO adviseert de verantwoordelijke voor het informatiesysteem of het informatieproces, althans de organisatie, waarop de maatregelen van toepassing zijn hierover. De CISO werkt aan de bewustwording van de beveiliging van informatiesystemen in samenwerking met de beveiligingsautoriteit van het ministerie; het informatiebeveiligingsbewustzijn is een aanvulling op de bewustwording van integrale beveiliging. Zo informeert de CISO de beveiligingsautoriteit regelmatig over digitale dreigingen en informatiebeveiligingsrisico's, opdat in samenwerking hierop kan worden gereageerd en de dreiging of het risico kan worden verkleind of weggenomen.

De CISO ontwikkelt beleid of de kaders en richtlijnen op het gebied van informatiebeveiliging, indien hij of zij dat gegeven de digitale dreigingen en informatiebeveiligingsrisico's in het ministerie nodig acht. De CISO houdt hierbij rekening met de strategische visie van de CIO op de digitale transformatie, zoals dat is verwoord in het meerjarige departementale informatieplan. Het behoort vervolgens tot de taak van de CISO om ervoor te zorgen dat deze kaders of richtlijnen door het lijnmanagement dat verantwoordelijk is voor de informatiesystemen en diensten duurzaam worden geïmplementeerd. Hiervoor ontwikkelt en coördineert hij of zij de benodigde activiteiten die de informatiebeveiliging in het departement bevorderen. De CISO ontwikkelt daarnaast een risicobeeld, hij of zij inventariseert daarvoor de informatiebeveiligingsrisico en voorziet deze van een beoordeling. De CISO houdt dit risicobeeld actueel. Op basis van het risicobeeld kan de CISO vervolgens in het portfolio informatiebeveiliging de nieuwe, en wijzigingen in al in productie zijnde, informatiesystemen in zijn of haar organisatie prioriteren. Deze prioritering draagt ertoe bij om de informatiebeveiligingsrisico's uit het risicobeeld efficiënt te verkleinen en digitale dreigingen af te wenden. Daarnaast zijn er informatiebeveiligingskaders en -richtlijnen die gelden voor alle ministeries, bijvoorbeeld de Baseline Informatiebeveiliging Overheid. Het is de taak van de CISO om het lijnmanagement dat verantwoordelijk is voor de betreffende informatiesystemen in de organisatie te adviseren hoe deze kaders en richtlijnen in het concrete geval het beste kunnen worden toegepast.

In samenspraak met de CIO is de CISO belast met de continue ontwikkeling van het rijksbrede beleid op het gebied van informatiebeveiliging en privacy van informatiesystemen en diensten. Het betreft hier de meerjarige I-strategie van CIO Rijk, het risicobeeld en het calamiteitenplan van CISO Rijk. Ook draagt de CISO bij aan het integrale beveiligingsbeleid, de departementale analyse van beveiligingsrisico's die de beveiligingsautoriteit opstelt en het calamiteitenplan, bedoeld in het Besluit BVA-stelsel Rijksdienst 2021.

Voor de ontwikkeling van het rijksbrede beleid op het gebied van informatiebeveiliging is het uitgangspunt van het versterken van het lerend vermogen door kennisdeling en het onderhouden van relaties belangrijk. In dit verband onderhoudt de CISO met regelmaat het contact met de inlichtingen- en veiligheidsdiensten, het Nationaal Cyber Security Centrum (NCSC) en de Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV). Er wordt in die verhoudingen informatie en kennis uitgewisseld over dreigingen die verband houden met de informatiebeveiliging van het departement. Hij of zij adviseert en informeert de CISO Rijk, voor zover dit redelijkerwijs noodzakelijk is voor de uitoefening van diens taken, en de beveiligingsautoriteit hierover gevraagd en ongevraagd voor hun taakuitoefening op grond van dit besluit respectievelijk het Besluit BVA-stelsel Rijksdienst 2021. Zijn of haar adviezen zijn onder meer op basis van zijn of haar risicobeeld, het departementale informatieplan en zijn of haar kennis van en ervaring met het ontwikkelen van departementaal beleid op het gebied van informatiebeveiliging. Voor het onderhouden van de relaties met de inlichtingen- en veiligheidsdiensten, de NCSC en de NCTV is een verklaring van geen bezwaar vereist.

Tot slot levert een CISO de bijdrage op het gebied van informatiebeveiliging aan de beoordeling van de beheersbaarheid, de slaagkans en de risico's van wijzigingen in informatiesystemen en diensten met een grote meerjarige ICT-component. Dit gebeurt door middel van een bijdrage aan het verplichte

CIO-oordeel. De bijdrage gaat met name in op het risicomanagement op het gebied van informatiebeveiliging van alle voorgenomen en in uitvoering zijnde ICT-wijzigingen aan informatiesystemen. Verder monitort en signaleert de CISO bij zelfstandige bestuursorganen eventuele afwijkingen van artikel 41, eerste lid, van de Kaderwet zelfstandige bestuursorganen. In dit artikel is bepaald dat zelfstandige bestuursorganen zorg dragen, op de voet van de ter zake voor de rijksdienst geldende voorschriften, voor de nodige technische en organisatorische voorzieningen ter beveiliging van zijn gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens. De CISO voert deze taak gericht uit in die gevallen dat significante risico's of een feitelijke inbreuk op deze beveiliging gesignaleerd of geconstateerd zijn, zoals tijdens, of in de nasleep van, rijksbrede informatiebeveiligings-incidenten. De CISO informeert de secretaris-generaal, als eigenaar van het zelfstandig bestuursorgaan, over geconstateerde afwijkingen. Deze afwijkingen worden periodiek besproken in de CISO-raad om zo een algemeen beeld te verkrijgen van de geconstateerde afwijkingen.

### *Artikel 8 (Bevoegdheden departementale CISO)*

Het eerste lid beschrijft de mogelijkheid van de CISO om de secretaris-generaal en het verantwoordelijk lijnmanagement rechtstreeks te informeren. Het rechtstreeks informeren houdt in dat de CISO zonder tussenkomst van zijn of haar ambtelijke leiding of andere dienstonderdelen van het ministerie de secretaris-generaal of het verantwoordelijk lijnmanagement kan informeren. Deze mogelijkheid wordt, indien mogelijk, pas toegepast nadat overleg met de CIO of de beveiligingsautoriteit van het ministerie heeft plaatsgevonden. Indien dit niet mogelijk is, vindt het overleg zo spoedig mogelijk achteraf plaats. In de praktijk is deze mogelijkheid dan ook een ultimum remedium. Voordat van deze mogelijkheid gebruik gemaakt kan worden moet er namelijk een feit geconstateerd zijn dat een acuut risico op de veiligheid van de informatie binnen de rijksdienst met zich brengt.
Naast het rechtstreeks informeren van de secretaris-generaal is het ook van belang dat de CISO rechtstreeks informatie kan uitvragen over aangelegenheden die voor de uitoefening van zijn of haar taken nodig is. Het tweede lid strekt hiertoe. Het gaat bijvoorbeeld om het uitvragen van inlichtingen over de informatiebeveiliging van een bepaald informatiesysteem of het geheel van informatiesystemen in de vorm van een projectportfolio informatiebeveiliging, zoals bedoeld in artikel 7, onderdeel j.
Het derde lid regelt de bevoegdheid van de CISO om aanwijzingen te geven met betrekking tot de informatieprocessen binnen het ministerie. Hij of zij doet dit namens de secretaris-generaal en de departementale CIO. Het is een vergaande bevoegdheid en dient daarom aan voorwaarden te voldoen. Ingrijpen is alleen toegestaan als er sprake is van een ernstige en acute inbreuk op de beveiliging van informatiesystemen of er sprake is van een risico daarop. De CISO kan laten ingrijpen met maatregelen die de beveiliging herstellen, of zo goed mogelijk herstellen. De CISO kan ook laten ingrijpen met maatregelen die de schade die door de inbreuk ontstaat te herstellen en verdere schade voorkomen.

Het vierde lid geeft de CISO de bevoegdheid om aanwijzingen te geven aan iedere ambtenaar, externe medewerker en bezoeker voor zover dat noodzakelijk is voor de uitvoering van het departementale informatiebeveiligingsbeleid en de naleving van de voorschriften daarvan. Hij of zij geeft die aanwijzingen namens de secretaris-generaal van het ministerie en de departementale CIO onder wie hij of zij ressorteert. De CISO geeft die aanwijzingen in afstemming met de beveiligingsautoriteit van het departement.

### *Artikel 9 (Departementaal CIO-stelsel)*

Het eerste lid regelt dat voor dienstonderdelen van een ministerie met een substantieel portfolio van informatiesystemen er een CIO dient te worden aangesteld. De keuze om hiertoe over te gaan is aan de minister die verantwoordelijk is voor de leiding van een ministerie. Het vierde lid van dit artikel regelt op eenzelfde wijze dat er een CISO bij dergelijke dienstonderdelen wordt aangesteld.

Het tweede lid brengt tot uitdrukking dat de taken en bevoegdheden van de CIO van een dienstonderdeel een afgeleide zijn van die van de CIO op departementaal niveau. Het betreft dan een verantwoordelijkheid voor het beleid op en het zorgdragen voor de ontwikkeling en het beheer van de digitalisering en informatievoorziening van het dienstonderdeel. Daarbij moet opgemerkt worden dat de specifieke CIO-taken op het niveau van dienstonderdelen wel kunnen verschillen van de taken op departementaal niveau, afhankelijk van de organisatiecontext.

De digitalisering binnen de publieke taak van de ministeries neemt toe. De CIO van een dienstonderdeel is daarom onderdeel van de ambtelijke leiding van dat dienstonderdeel, omdat zijn of haar strategische visie ten aanzien van het anticiperen en implementeren van digitale ontwikkelingen - de digitale transformatie - de verschillende uitvoeringsdoelen en taakvelden van dat dienstonderdeel kunnen raken. Van deze bepaling kan beargumenteerd worden afgeweken (op grond van artikel 17 van dit besluit).

Het vijfde lid is vergelijkbaar met het tweede lid en brengt tot uitdrukking dat de taken en bevoegdheden van een CISO van een dienstonderdeel een afgeleide zijn van die van de departementale CISO. Het betreft dan een verantwoordelijkheid voor het informatiebeveiligingsbeleid, zoals bedoeld in artikel 3 van het Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007 en artikel 3 van het Besluit Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie 2013, voor zover dit betrekking heeft op dat dienstonderdeel. Ook moet hierbij opgemerkt worden dat de specifieke CIO-taken op het niveau van dienstonderdelen wel kunnen verschillen van de taken op departementaal niveau, afhankelijk van de organisatiecontext.

Het zesde lid brengt de verhouding binnen het departementale CIO-stelsel tot uitdrukking. De departementale CIO en de departementale CISO nemen in hun onderlinge verhouding een centrale positie in het stelsel en ten opzichte van de ambtelijke leiding in het ministerie in. Een CIO en een CISO bij een dienstonderdeel maken deel uit van dat departementale CIO-stelsel. Op grond van artikel drie, derde lid, is de departementale CIO namens de minister die verantwoordelijk is voor de leiding van het ministerie belast met de taak dat departementale stelsel in te richten. De verhouding van de departementale CIO ten opzichte van het stelsel komt verder tot uitdrukking in de mogelijkheid om informatie uit te vragen bij CIO's en CISO's van dienstonderdelen, zoals omschreven in artikel 5, vierde lid.

### *Artikel 10 (CIO Rijk en CISO Rijk)*

In eerste lid wordt geregeld dat de Minister van Binnenlandse Zaken en Koninkrijksrelaties de CIO Rijk en de CISO Rijk benoemt en ontslaat. Op deze wijze kan door de Minister van Binnenlandse Zaken en Koninkrijksrelaties invulling worden gegeven aan de vereiste competenties voor beide functies en wordt mede de coördinerende taak van de Minister van Binnenlandse Zaken en Koninkrijksrelaties voor het beleid betreffende de informatievoorziening van de rijksdienst tot uiting gebracht.

Het tweede lid belegt de coördinerende taak van de Minister van Binnenlandse Zaken en Koninkrijksrelaties voor het informatiebeleid van de rijksdienst bij de CIO Rijk. De CIO Rijk is belast met de ontwikkeling en coördinatie van het rijksbrede beleid voor de digitalisering. Voorts is de CIO Rijk belast met het zorg dragen voor de ontwikkeling en het beheer van de informatiesystemen en de informatievoorziening van de rijksdienst. Het lid sluit daarmee tevens uit dat de CIO Rijk een verantwoordelijkheid heeft voor de informatiesystemen van individuele departementen.

Het derde lid geeft uitdrukking en invulling aan het feit dat de CISO Rijk ressorteert onder de CIO Rijk. De CISO Rijk is belast met de coördinatie van het informatiebeleidsaspect informatiebeveiliging, dat betrekking heeft op digitale dreigingen en informatiebeveiliging voor zover deze betrekking hebben op de rijksdienst. Het derde lid belegt zodoende de coördinatie rondom informatiebeveiligingsbeleid bij de CISO Rijk.

### *Artikel 11 (Taken CIO Rijk)*

In dit artikel staan de taken benoemd waarmee de CIO Rijk belast is. De digitale trends die elkaar snel opvolgen maken dat het belang van een goede, meerjarige strategische visie op de digitale transformatie van de gehele rijksdienst komt. De taken uit dit artikel bepalen wat de taak van de CIO Rijk, zoals bedoeld in artikel 10, tweede lid, inhoudt.

De digitale transformatie waarmee een ministerie anticipeert op de (actuele) digitale ontwikkelingen en dreigingen sluiten aan op de meerjarige I-strategie voor de rijksdienst. Het is de taak van de CIO-Rijk om de CIO's in het CIO-stelsel te stimuleren daarmee gezamenlijk de digitale transformatie bij de rijksdienst, zoals verwoord in de meerjarige I-strategie, te verwezenlijken. Het is de taak van de CIO Rijk om alle functionarissen in het CIO-stelsel zo goed mogelijk in staat te stellen de technologisch gedreven innovaties te kunnen doen implementeren in overeenstemming met hun eigen visie op de digitale transformatie en met de meerjarige I-strategie. De CIO Rijk heeft hier binnen de hele rijksdienst de rol van een digitaal leider voor de rijksdienst. Hij of zij is niet alleen actief betrokken bij de digitale transformatie van de rijksdienst, maar bevordert ook het lerend vermogen binnen het CIO-stelsel in de rijksdienst, onder andere door kennisdeling. Daarbij moet in het bijzonder gedacht worden aan het investering in een actieve samenwerking met kennisinstituten en het bedrijfsleven. De kennis en de kansen om adequaat te anticiperen op die digitale ontwikkelingen of dreigingen worden daar in veel gevallen gecreëerd. Dat biedt mogelijkheden voor de rijksdienst en het CIO-stelsel daarin en het is de taak van de CIO Rijk om die kennis en kansen maximaal te benutten voor het CIO-stelsel als geheel en de relevante actoren in het CIO-stelsel daarvan te overtuigen. Interdepartementale overleggen, zoals het CIO-beraad en de CISO-raad, kunnen vervolgens de plek zijn om deze opgedane kennis en inzichten ook buiten de organisatie, maar binnen de rijksdienst, te delen.

Nu digitalisering een integraal onderdeel vormt van de bedrijfsvoering of het primaire proces in

overheidsorganisaties is het belangrijk dat de CIO Rijk de Minister van Binnenlandse Zaken en Koninkrijksrelaties adviseert. Hij of zij adviseert de minister en het lijnmanagement van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties over de gevolgen voor het rijksbrede informatiebeleid, de informatiesystemen en informatieprocessen van de rijksdienst van onder andere (voorgenomen) wet- en regelgeving, beleid, uitvoeringstrajecten en investeringen voor zover die een brede impact hebben op de rijksdienst, daarbij gebruikt hij of zij de meerjarige I-strategie. Hij of zij betrekt in dit advies indien nodig de CISO Rijk. De meerjarige I-strategie bevat de beleidsprioriteiten voor de informatiesystemen en de informatievoorziening van de rijksdienst, zoals in artikel 10, tweede lid bedoeld. Elke prioriteit kent een meerjarige planning en wordt per prioriteit beargumenteerd van de financiële gevolgen voorzien. De prioriteiten en de financiële onderbouwing ervan worden elk jaar bijgewerkt in overleg met het CIO-beraad en anticiperen op technologische ontwikkelingen en digitale trends. De bijgewerkte meerjarige I-strategie wordt door de Minister van Binnenlandse Zaken en Koninkrijksrelaties vastgesteld en jaarlijks naar de Tweede Kamer der Staten-Generaal gezonden.

De CIO Rijk heeft verder de taak om kaders te ontwikkelen ter bevordering van de eenheid, de kwaliteit of de efficiëntie van alle informatiesystemen bij de rijksdienst. Het betreft hier kaders die zowel betrekking kunnen hebben op informatiesystemen ten behoeve van de interne huishouding van een organisatie binnen de rijksdienst als ook informatiesystemen die aan te merken zijn als bedrijfsprocessen met een op externe (op derden gerichte) werking. Ook is de CIO Rijk belast met de taak om kaders op te stellen voor de wijze waarop de gegevens over de informatiesystemen worden verstrekt. Hierbij kan gedacht worden aan kaders over het format, de frequentie en de tijdstippen waarop gegevens worden aangeleverd, zoals gegevens met betrekking tot het installeren van updates in het kader van informatiebeveiliging; het levenscyclusmanagement van informatiesystemen en het portfoliobeheer. De kaders die de CIO Rijk heeft opgesteld worden bijgesteld of aangescherpt op basis van een regelmatige analyse (van de trends in) de informatie die de CIO Rijk ontvangt op grond van artikel 6, eerste lid van het Coördinatiebesluit. De analyses en de aandachtspunten uit de analyses van die informatie worden gedeeld met het CIO-beraad met als doel de eenheid, kwaliteit en efficiëntie van informatiesystemen binnen de rijksdienst te bevorderen. De Minister van Binnenlandse Zaken en Koninkrijksrelaties stelt deze kaders, na opstelling, bijstelling of aanscherping, uiteindelijk vast.

De CIO Rijk heeft eveneens de taak het hoofdstuk over de informatievoorziening binnen de rijksdienst in de jaarrapportage bedrijfsvoering rijksdienst voor te bereiden. In dat hoofdstuk komen belangrijke onderdelen aan bod met betrekking tot de digitalisering, informatievoorziening en informatiesystemen en de informatievoorziening binnen het rijk. Activiteiten met een grote ICT-component, de kosten voor grote wijzigingen van informatiesystemen en diensten binnen de rijksdienst evenals de naleving van de op grond van artikel 2, eerste lid, en 6, tweede lid van het Coördinatiebesluit gestelde kaders komen hierin jaarlijks aan bod.

Tot slot is het de taak van CIO Rijk om, in overleg met de departementale CIO, te evalueren in welke mate de departementale informatieplannen van de CIO's passen binnen de beleidsprioriteiten van de meerjarige I-strategie van CIO Rijk of daar invulling aan geven, en aansluiten bij gestelde kaders op grond van het Coördinatiebesluit. De CIO Rijk rapporteert hierover aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties. De prioritaire doelstellingen uit het meerjarige departementale informatieplan kunnen aanleiding zijn voor het aanvragen van een advies bij het Adviescollege ICT-toetsing. Voorts is het de taak van de CIO Rijk om toe te zien op de naleving van de vastgestelde kaders zoals bedoeld in artikel 2, eerste lid, en 6, tweede lid, van het Coördinatiebesluit.

***Artikel 12 (Bevoegdheden CIO Rijk)***

Het eerste lid beschrijft de mogelijkheid van de CIO Rijk om, na overleg met de secretaris-generaal van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, de Minister van Binnenlandse Zaken en Koninkrijksrelaties rechtstreeks te informeren als zijn of haar taakuitoefening, zoals uiteengezet in het vorige artikel, hiertoe aanleiding geeft. Het rechtstreeks informeren houdt in dat de CIO Rijk zonder tussenkomst van de ambtelijke leiding of andere dienstonderdelen van het ministerie de Minister van Binnenlandse Zaken en Koninkrijksrelaties kan informeren, indien zijn of haar taken, op grond van artikel 10, hiertoe aanleiding geven. Deze mogelijkheid wordt toegepast nadat overleg met de secretaris-generaal van het ministerie heeft plaatsgevonden. In de praktijk is deze mogelijkheid dan ook een ultimum remedium. Ingeval het ministerie van Binnenlandse Zaken en Koninkrijksrelaties door meer dan één bewindspersoon wordt geleid, betreft het de bewindspersoon die de rijksdienst, specifiek CIO Rijk, in zijn of haar portefeuille heeft.

In het tweede lid wordt geregeld dat de CIO Rijk, namens de minister van Binnenlandse Zaken en Koninkrijksrelaties, het overleg over de benoeming en ontslag van een CIO van een ministerie, bedoeld in artikel 3a Coördinatiebesluit. Op deze wijze kan door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties advies over onder meer de invulling van vereiste competenties worden geleverd en wordt mede de coördinerende taak van de minister van Binnenlandse Zaken en Konink-

rijksrelaties voor het beleid betreffende de informatievoorziening van de rijksdienst tot uiting gebracht.

***Artikel 13 (Taken CISO Rijk)***

In dit artikel staan de taken benoemd waarmee de CISO Rijk belast is. De CISO Rijk vult met deze taken een deel van de taken van de CIO Rijk in. Naast de digitale trends ontwikkelen ook de digitale dreigingen en de risico's op informatiebeveiliging zich. De CISO Rijk zal vanuit de in dit artikel genoemde taken continu moeten anticiperen op deze ontwikkelingen en informatiebeveiligingsincidenten die de Rijksdienst raken coördineren.

De CISO Rijk adviseert over de digitale dreigingen en risico's met betrekking tot informatiebeveiliging, deze kunnen altijd een impact hebben op de bedrijfsvoering of het primaire proces in de gehele rijksdienst. De CISO Rijk adviseert hierover aan het lijnmanagement en de CIO Rijk over die risico's en dreigingen en over de gevolgen van (voorgenomen) wet- en regelgeving, beleid, uitvoeringstrajecten en investeringen bettrekking hebben op de rijksdienst. De CISO Rijk gebruikt hierbij het onderdeel over de informatiebeveiliging in de meerjarige I-strategie. De inzichten over informatiebeveiliging en ook de actuele trends en digitale dreigingen daarin kan de CISO Rijk ook gevraagd en ongevraagd gebruiken voor advies voor of delen met de CISO's, de beveiligingsautoriteit Rijk en de CISO's van andere dienstonderdelen van de ministeries. Het doel is om concrete informatiesystemen binnen de rijksdienst beter te beschermen tegen incidenten en calamiteiten op het gebied van informatiebeveiliging. De kennisdeling van de CISO Rijk versterkt daarmee het vermogen in het CIO-stelsel om snel te leren en op basis van die kennis te anticiperen op digitale dreigingen.

De CISO Rijk ontwikkelt en coördineert het beleid of de kaders op het gebied van informatiebeveiliging, indien hij of zij dat gegeven de digitale dreigingen en informatiebeveiligingsrisico's in rijksdienst nodig acht. De CISO houdt hierbij rekening met de strategische visie van de CIO Rijk op de digitale transformatie en de informatievoorziening, zoals dat is verwoord in de meerjarige I-strategie. De CISO Rijk zorgt er vervolgens voor dat het rijksbrede beleid en de kaders over digitalisering en informatievoorziening, op het onderdeel informatiebeveiliging duurzaam geïmplementeerd wordt binnen de rijksdienst. Dit moet begrepen worden op zowel technische als organisatorische aard. De CISO Rijk draagt in dat verband dan ook zorg voor bijvoorbeeld de noodzakelijke cultuurveranderingen in de rijksdienst voor zover het de informatiebeveiliging betreft. Hiervoor coördineert de CISO Rijk ook de wijze waarop de gegevens over de informatiebeveiliging van informatiesystemen door de ministeries worden verstrekt conform de bedoeling van het Coördinatiebesluit.

Daarnaast ontwikkelt, coördineert en monitort de CISO Rijk de naleving van het rijksbrede informatiebeveiligingsbeleid met behulp van een rijksbreed risicobeeld. Voor dat risicobeeld inventariseert de CISO Rijk de informatiebeveiligingsrisico's en voorziet deze van een beoordeling. Het stelt dit risicobeeld op, onder andere aan de hand van de departementale risicobeelden, bedoeld in artikel 7, onderdeel c, en zijn of haar contact met de inlichtingen- en veiligheidsdiensten, de NCSC en de NCTV. Dat contact met de laatste organisatie onderhoudt hij of zij regelmatig om een goed beeld te houden voor de dreingingen die verband houden met de informatiebeveiliging van de rijksdienst en onder andere van nut kunnen zijn voor het actueel houden van het rijksbrede risicobeeld door de CISO Rijk. Voor het onderhouden van de relaties met de inlichtingen- en veiligheidsdiensten, de NCSC en de NCTV is voor de CISO Rijk een verklaring van geen bezwaar vereist. Voor dit rijksbrede risicobeeld werkt de CISO Rijk samen met de CISO's en de beveiligingsautoriteit Rijk. Aan de hand van dit risicobeeld monitort de CISO Rijk de naleving in de rijksdienst van de op grond van het Coördinatiebesluit gestelde informatiebeveiligingskaders, zoals de Baseline Informatiebeveiliging Overheid en brengt die, indien nodig, ter sprake de CISO-raad. Het is hierbij de taak van de CISO Rijk om te bewerkstelligen dat organisaties die deel uit maken van het CIO-stelsel Rijksdienst zich bewust zijn van digitale dreigingen en de risico's van informatiebeveiliging en dat dit bewustzijn wordt vergroot. Tot slot stelt de CISO Rijk samen met hen het calamiteitenplan, bedoeld in het Besluit BVA-stelsel Rijksdienst 2021, op voor zover dit betrekking heeft op de informatiebeveiliging.

De CISO Rijk formuleert daarnaast de beleidsprioriteiten van het onderdeel informatiebeveiliging van de meerjarige I-strategie, dat gaat over de beveiliging van de informatiesystemen van de rijksdienst, elke prioriteit kent een meerjarige planning en wordt per prioriteit beargumenteerd van de financiële gevolgen voorzien. De prioriteiten en de financiële onderbouwing ervan worden elk jaar bijgewerkt in overleg met de CISO-raad, voorafgaand aan het CIO-beraad. Het onderdeel informatiebeveiliging van de meerjarige I-strategie anticipeert op digitale dreigingen en informatiebeveiligingsrisico's voor informatiesystemen binnen de rijksdienst. De bijgewerkte meerjarige I-strategie wordt door de Minister van Binnenlandse Zaken en Koninkrijksrelaties jaarlijks vastgesteld en naar de Tweede Kamer der Staten-Generaal gezonden. De CISO Rijk coördineert de aanpak van rijksbrede informatiebeveiligingsincidenten en -calamiteiten. Op het moment dat er een informatiebeveiligingsincident is dat informatiesystemen in de rijksdienst raakt, dan verzamelt de CISO Rijk bij alle betrokken organisaties in de rijksdienst alle informatie hierover die hij of zij daartoe nodig acht. Hij of zij gebruikt deze

informatie om in samenwerking met de CISO-raad, de CIO Rijk en de beveiligingsautoriteit Rijk tot beslissingen te komen die het incident of de calamiteit stoppen en de schade aan informatiesystemen en het verlies of de ongewenste verspreiding van informatie tot een minimum beperken.

***Artikel 14 (Bevoegdheden CISO Rijk)***

Het eerste lid van dit artikel regelt dat de CISO Rijk de secretaris-generaal van het ministerie van Binnenlandse Zaken en Koninkrijksrelatie en het verantwoordelijk lijnmanagement in de nodige gevallen rechtstreeks kan informeren, dus zonder tussenkomst van zijn of haar ambtelijke leiding. Het betreft een bevoegdheid die in uitzonderlijke gevallen wordt gebruikt door de CISO Rijk binnen de grenzen van zijn of haar taken op grond van dit besluit. De uitzonderlijkheid moet in die zin begrepen worden dat er dan sprake is van een acuut risico op het verlies van gegevens of schade aan informatiesystemen die de bedrijfscontinuïteit van de rijksdienst ernstig belemmeren of onmogelijk maken. Als overleg met de CIO Rijk en de beveiligingsautoriteit Rijk vooraf niet mogelijk is, gebeurt dit zo spoedig mogelijk daarna.

De CISO Rijk heeft een coördinerende rol bij de aanpak van rijksbrede informatiebeveiligingsincidenten en -calamiteiten. Het tweede lid regelt dit. Het betreft dan een hoog en acuut risico op een inbreuk op de informatiebeveiliging met een rijksbreed karakter. De inbreuk overstijgt daarmee het departementale niveau. In die coördinatierol kan de CISO Rijk, na afstemming met de betreffende departementale CISO's aanwijzingen geven aan iedere ambtenaar, externe medewerker en bezoeker met betrekking tot de informatieprocessen van ministeries. Ook kan de CISO Rijk onmiddellijk de maatregelen laten treffen die hij of zij nodig acht om het verlies van gegevens of de schade aan informatiesystemen zo veel mogelijk te beperken. De afstemming met de departementale CISO's is hierbij een noodzakelijke processtap omdat de risicocontext per ministerie sterk kan verschillen. Zo kan een aanwijzing om bepaalde software per direct niet meer te gebruiken in sommige gevallen een onevenredig zware impact hebben op de (maatschappelijke) belangen die met de betreffende informatieprocessen gediend worden. Met inachtneming van deze organisatie-specifieke context hebben de aanwijzingen van de CISO Rijk nadrukkelijk een 'pas toe of leg uit'-karakter. Indien een aanwijzing van de CISO Rijk niet - in het geheel of met onmiddellijke ingang - kan worden opgevolgd, treft de departementale CISO op basis van diens eigen bevoegdheden onder artikel 8, lid 2 en 4, passende maatregelen in de geest van de betreffende aanwijzing. De CISO rapporteert de interne afweging en de getroffen maatregelen dan per ommegaande aan de CISO Rijk. De CISO Rijk kan ook zelf, bij alle betrokken organisaties in de rijksdienst, de informatie verzamelen die hij of zij bij de uitoefening van de coördinerende rol nodig acht. Hij of zij treedt zo spoedig mogelijk in overleg met de CISO's van de betrokken departementen, de CIO Rijk en de beveiligingsautoriteit Rijk om tot beslissingen te komen. De CISO Rijk beschikt in dit verband ook over een bevoegdheid om indien nodig direct toegang tot de secretaris-generaal van dat departement te krijgen. Ook de directe toegang tot de secretaris-generaal hanteert de CISO Rijk alleen in afstemming met de CISO van het betrokken departement.

***Artikel 15 (CIO-beraad)***

Het eerste lid regelt dat de Minister van Binnenlandse Zaken en Koninkrijksrelaties een CIO-beraad instelt. Het CIO-beraad is een vooroverleg van de Interdepartementale Commissie Bedrijfsvoering Rijksdienst en bespreekt op strategisch niveau de digitale transformatie van de gehele rijksdienst om de eenheid, kwaliteit en efficiëntie van informatiesystemen binnen de rijksdienst te verbeteren. Het digitaal leiderschap van de leden van het CIO-beraad leidt ertoe dat de invloed van technologisch gedreven innovaties op de informatiesystemen goed wordt ingeschat. Daarop wordt in gezamenlijk overleg geanticipeerd, onder andere door middel van het ontwikkelen en implementeren van de meerjarige I-strategie. Het CIO-beraad coördineert zo centraal en in gezamenlijk overleg de digitale transformatie van de rijksdienst. Dat de CIO Rijk het CIO-beraad voorzit, wordt in het tweede lid geregeld.

Het derde lid omschrijft de leden van het CIO-beraad. Daar nemen ten minste alle departementale CIO's aan deel. Het staan hen geheel vrij om in gezamenlijk overleg te bepalen wie zij nog meer aan het CIO-beraad willen laten deelnemen. Het CIO-beraad stelt hiertoe een handvest op dat in ieder geval bepaalt wat de voorwaarden zijn voor deelname aan het CIO-beraad en wat de wijze van vergaderen is. Dit handvest wordt tweejaarlijks geactualiseerd.

Het vijfde lid en de daaropvolgende leden regelen de voorportalen van het CIO-beraad. De CISO-raad is een voorportaal van het CIO-beraad en heeft alleen betrekking op het informatiebeveiligingsbeleid van de rijksdienst. De CISO-raad bereidt het opstellen van informatiebeveiligingskaders binnen de rijksdienst voor, zoals de Baseline Informatiebeveiliging Overheid. Eveneens bespreekt de CISO-raad het onderdeel informatiebeveiliging van de meerjarige I-strategie. Het zesde lid regelt dat de CISO Rijk de CISO-raad voorzit en dat daaraan ten minste departementale CISO's deelnemen. De Chief Techno-

logy Officer-raad (CTO-raad) functioneert op het gebied van ICT-aanbodsturing en informatietechnologie. Het zevende lid regelt dat de CTO-raad wordt voorgezeten door de CIO Rijk. Aan de CTO-raad nemen ten minste de directeuren van de ICT-dienstverleners binnen de rijkdienst als lid deel. Het Tactisch Overleg Rijksnetwerken (TORN) functioneert op het gebied van ontwikkeling, implementatie en beheer van de Rijksnetwerken. Het achtste lid regelt dat het TORN wordt voorgezeten door een afgevaardigde van de CIO Rijk. Aan het TORN nemen ten minste deel de afgevaardigden van de ICT-dienstverleners binnen de rijksdienst en afgevaardigden van de departementale CIO-offices. Het Tactisch Overleg Rijksbrede Voorzieningen (TORV) functioneert als voorportaal van het CIO-beraad op het gebied van Rijksbrede ICT-voorzieningen. Het negende lid regelt dat het TORV wordt voorgezeten door een afgevaardigde van de CIO Rijk. Aan het TORV nemen ten minste deel de afgevaardigden van de CIO-offices.

***Artikel 16 (Rijks ICT-dashboard)***

Het eerste lid regelt dat er een Rijks ICT-dashboard is. In het tweede lid staat beschreven dat het Rijks ICT-dashboard alle grote voorgenomen nieuwe en grote wijzigingen binnen bestaande informatiesystemen en diensten bij ministeries en uitvoeringsorganisaties bevat. Het doel van het Rijks ICT-dashboard is het inzichtelijk maken van aantallen, kosten en de voortgang van ICT-wijzigingen met een meerjarige ICT-component van tenminste vijf miljoen euro. Onderhoud- en beheeractiviteiten zullen in toenemende mate op het ICT-dashboard zichtbaar zijn. Voornoemde inzichtelijkheid geldt met name voor de Staten-Generaal ten behoeve van de controlerende taak, maar ook om de transparantie naar de burger te vergroten en tot slot draagt de inzichtelijkheid van deze informatie bij aan het lerend vermogen in het CIO-stelsel.

De CIO Rijk beheert het Rijk ICT-dashboard op basis van de in het vierde lid van dit artikel aangeleverde informatie. De regels op basis waarvan de CIO Rijk het Rijks ICT-dashboard beheert, staan onder meer omschreven in het jaarlijks geactualiseerde kader Portfoliomanagement Rijk; voorheen het Handboek Portfoliomanagement Rijk.

In het vierde lid wordt de verantwoordelijkheid van de ministers omschreven voor het actualiseren van het ICT-dashboard en de kwaliteit van de gegevens van zijn of haar departement en de betrokken uitvoeringsorganisaties.

***Artikel 17 (Uitzonderingen)***

De bepalingen in dit besluit bewerkstelligen een hechtere interdepartementale samenwerking waarmee de rijksdienst wendbaarder wordt ten aanzien van digitale ontwikkelingen en weerbaarder wordt tegen digitale dreigingen. Elke organisatie zal haar eigen inspanning moeten leveren en aanpassing moeten doen om aan de bepalingen uit de besluit tegemoet te kunnen komen. De beschrijving van onder meer de taken en bevoegdheden van de CIO en de CISO in dit besluit moet gezien worden als een groeimodel en het kan niet verwacht worden dat na de inwerkingtreding van dit besluit alle organisaties binnen de rijksdienst kunnen voldoen aan de in dit besluit gestelde bepalingen. Om die reden biedt deze bepaling de mogelijkheid voor de ministers die belast zijn met de leiding van een ministerie op onderdelen af te wijken van het bepaalde in dit besluit. Er kan afgeweken worden wanneer dit de effectiviteit van de met dit besluit beoogde doelen ten goede komt en dit geschiedt na overleg met de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

***Artikel 18 (Evaluatie)***

Het artikel regelt dat er drie jaar na de inwerkingtreding van het besluit, en vervolgens om de drie jaren, een evaluatie van dit besluit plaatsvindt. In deze evaluatiebepaling komt ook het groeimodel van dit besluit CIO-stelsel tot uitdrukking. Ontwikkeling van dit besluit, op basis van de ervaringen over de werking van het CIO-stelsel rijksdienst, kan met deze evaluatiebepaling eens in de drie jaar plaatsvinden. Het besluit is daarmee op zichzelf ook een uiting van de digitale transformatie van de rijksdienst.

*De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,*
*R.W. Knops*