





Rijksoverheid

Menu 

## Chief Information Security Officer

Nationaal Cyber Security Centrum



Den Haag - [route](#) 



Universitair Master



36 uur



schaal 13

€5.212 - €7.747 (bruto)



ICT



Solliciteer voor 13 oktober 2024



Arbeidsovereenkomst voor bepaalde tijd met  
uitzicht op onbepaalde tijd

Kenmerk: 55418, Plaatsingsdatum: 25 september 2024

**Functieomschrijving**



Als CISO ben jij verantwoordelijk voor onze eigen interne informatiebeveiliging en risicomanagement. Zo zorg je er voor dat de informatieverwerking van het NCSC veilig en ongestoord kan verlopen en lever je een bijdrage aan de digitale veiligheid van Nederland. Geïnteresseerd? Lees dan vooral verder!

### **Wat ga je doen?**

Als CISO bij het NCSC heb je een breed, afwisselend takenpakket waarin adviserende, coördinerende, organiserende en beleidsmatige aspecten worden gecombineerd. Je zorgt ervoor dat het NCSC de eigen informatiebeveiliging adequaat en op een volwassen wijze kan besturen. Je draagt bij aan visieontwikkeling op dit terrein, adviseert bij prioriteitstelling en de uitwerking in beveiligingsplannen en roadmaps. Vervolgens coördineer je de realisatie daarvan. Hiermee borg je dat de stappen die rondom informatiebeveiliging gezet worden, nauw aansluiten bij, en bijdragen aan, de strategische ambities, doelstellingen en positie van de organisatie. Je zorgt ervoor dat het risicomanagement proces, in het bijzonder ook op het gebied van informatiebeveiliging, goed en volwassen werkt. Je bent verantwoordelijk voor het ISM-proces en ISMS en ziet erop toe dat er een actueel overzicht van de Te Beschermen Belangen bestaat en dat er risicoanalyses worden uitgevoerd. Je hebt een management rol en bent verantwoordelijk voor het functioneren, aansturing en doorontwikkeling van het sterk groeiende CISO-office (5 FTE). Als onderdeel hiervan ben je verantwoordelijk voor de uitvoering van plannen, taken en activiteiten van het CISO-office en het management van budgetten, personeel en doelrealisatie (jaarplannen, Planning & Control e.d.).

Een greep uit jouw werkzaamheden:

- Om informatiebeveiliging op een juiste manier te kunnen doorontwikkelen dient de basis op orde te zijn en te blijven. De organisatie, maar ook onze omgeving, verwacht dat van ons en verwacht ook dat we dat kunnen laten zien. Compliance en assurance/certificering zijn daarmee belangrijk. Je zorgt ervoor dat de organisatie alle wettelijke, rijksbrede en departementale kaders op het gebied informatiebeveiliging op een juiste wijze heeft geïmplementeerd en dat deze aantoonbaar effectief functioneren. Hierbij kijk je verder dan alleen de eigen organisatie en bijvoorbeeld ook naar onze supply

chain. Tegelijk weet je dat compliance geen doel op zich is, maar een basis vereiste om op een juiste manier grip te houden op informatiebeveiliging.

- Je zorgt voor inzicht en overzicht op het vlak van incidenten, dreigingen, risico's, kwetsbaarheden e.d. daar waar het de eigen organisatie betreft. Je bent in die zin verantwoordelijk voor het opstellen en rapporteren op metrics en KPI's. Op basis daarvan zorg je ervoor dat inzichtelijk wordt hoe de informatiebeveiliging functioneert en waar we die hebben te veranderen. Je bent functioneel verantwoordelijk voor de aansturing van onze interne security monitoring en detectie voorzieningen. Je monitort of incidenten en oorzaken tijdig worden opgelost en adviseert de verantwoordelijke lijnonderdelen bij incident afhandeling.
- Je monitort en evalueert de effectiviteit van de interne informatiebeveiliging en stelt deze waar nodig bij zodat we onze informatiebeveiliging steeds op een hoger plan kunnen brengen. Je stimuleert binnen de wettelijke kaders, richtlijnen en risicobereidheid van de organisatie innovatie en vernieuwing.
- Je creëert bewustzijn en betrokkenheid binnen de organisatie op het brede terrein van informatiebeveiliging en risicomanagement. Daarnaast verzorg je externe presentaties en publicaties op je vakgebied en laat je zien wat de NCSC-visie en -werkwijze rondom informatiebeveiliging is. Je hebt daarmee ook extern een adviserende en gezichtsbepalende rol.

## Functie-eisen



### Wie ben jij?

Je bent een ervaren informatiebeveiligingsadviseur met enkele jaren ervaring als (plv.) CISO. Je weet hoe het is om CISO te zijn en beschikt over de visie en ambitie om deze rol invulling te kunnen geven. Het NCSC en onze dienstverlening optimaal kunnen laten functioneren vormt je drive. Je hebt daarom ook een sterke focus op de business impact van informatiebeveiliging(smaatregelen). Je denk niet alleen in risico's maar vooral ook in kansen, mogelijkheden en oplossingen. Het NCSC is een snel veranderende organisatie in een snel veranderende omgeving. Innovatie, verandersnelheid en flexibiliteit staan bij ons centraal. Dat vraagt wat van de gehele

organisatie, en ook zeker van de CISO en CISO Office. Je houdt van een dergelijke omgeving en kijkt er naar uit om onze initiatieven rondom bijvoorbeeld Shift-Left in Security, DevSecOps, veilige cloud adoptie en ML-gebruik, verder aan te jagen.

Je bent een overtuigende adviseur met krachtige adviesvaardigheden en een focus op resultaten. Behalve in het formuleren en uitdragen van een visie en oplossing ben je ook sterk in het vervolgens implementeren en werkend krijgen daarvan. Een visie, strategie en plan krijgt immers dan pas echt waarde.

De CISO werkt op strategisch, tactisch en soms ook op technisch/operationeel niveau. Je kunt daar snel tussen schakelen beschikt over de contactuele vaardigheden om effectief te kunnen communiceren op de verschillende niveaus en kunt omgaan met de verschillende belangen en zienswijzen in de organisatie, én daarbuiten. Je neemt initiatief, je bent overtuigend en gericht op samenwerken. Je bent analytisch sterk, omgevingsbewust en organisatie sensitief. Het NCSC is een overheidsorganisatie en onderdeel van het Ministerie van Justitie en Veiligheid. Je weet wat het behelst om in een grote concernsetting te werken en beschikt over een goed ontwikkelde bestuurlijke sensitiviteit. Je kunt uitstekend zakelijk schrijven en je beschikt over uitstekende communicatieve vaardigheden, zowel in het Nederlands als in het Engels.

### **Verder beschik je over:**

- WO-kennis en denkniveau, aangevuld met opleidingen certificeringen op het vlak van informatiebeveiliging of cybersecurity, zoals CISM of CISSP;
- Enkele jaren leidinggevende werkervaring en minimaal vijf jaar ervaring in vergelijkbare rollen op strategisch niveau als bijvoorbeeld CISO of plv/wnd-CISO. Bij voorkeur heb je die ervaring opgedaan in een middelgrote of grotere organisatie in de private sector of bij een uitvoeringsorganisatie van de overheid;
- Uitgebreide kennis van, en visie op, het vakgebied om de CISO om deze adequaat door te kunnen ontwikkelen;
- Je hebt succesvol veranderingen en verbeteringen gerealiseerd op het vlak van informatiebeveiliging in de organisaties waar je hebt gewerkt.
- Je hebt ervaring met de implementatie en toepassing van actuele CISO vraagstukken zoals rondom Shift-Left, DevSecOps, cloud security, information security automation

en ML/AI toepassingen.

## Arbeidsvoorwaarden



### Salarisniveau

schaal 13

### Maandsalaris

Min €5.212 – Max. €7.747 (bruto)

### Dienstverband

Arbeidsovereenkomst voor bepaalde tijd met uitzicht op onbepaalde tijd

### Contractduur

1 jaar

### Minimaal aantal uren per week

36

### Maximaal aantal uren per week

36

## Overige arbeidsvoorwaarden




Naast het salaris ontvang je een individueel keuzebudget (IKB). Het IKB bestaat uit geld (16,5% van je bruto jaarsalaris) en tijd. Met het IKB maak jij de keuzes die bij jou passen en kun je een deel van je arbeidsvoorwaarden zelf samenstellen. Je kunt er bijvoorbeeld voor kiezen om een deel van je maandinkomen te laten uitbetalen wanneer jij dat wenst. Ook kun je dit budget omzetten in verlof en andersom of besteden aan fiscaalvriendelijke doelen. De Rijksoverheid hecht sterk aan persoonlijke groei en loopbaanontwikkeling en biedt daarvoor tal van mogelijkheden. Tot de

secundaire arbeidsvoorwaarden behoren onder meer verschillende studiefaciliteiten, bedrijfsfitness, volledige vergoeding van je ov-reiskosten woon-werkverkeer en gedeeltelijk betaald ouderschapsverlof.

## Bijzonderheden



Solliciteren? Nadat je via de sollicitatiebutton hebt gereageerd kun je jouw cv en motivatie als word of pdf-bestand uploaden.

Het toetsen van de integriteit van onze nieuwe collega's is voor het NCSC van groot belang. Om die reden maakt een veiligheids A onderzoek onderdeel uit van het sollicitatieproces. De duur van het onderzoek zal minimaal 8 weken in beslag nemen. Meer informatie over het onderzoek kun je vinden op <https://www.aivd.nl/onderwerpen/veiligheidsonderzoek> .

Wanneer je als interne collega van de Rijksoverheid een beroep doet op een voorrangpositie, stuur dan ook een kopie van je beschikking mee.

Een assessment en/of vaardigheidstests kan deel uitmaken van het sollicitatieproces, net als het opvragen van referenties en het inzetten van een (online) screening.

Werken bij een crisisorganisatie vraagt om flexibiliteit van onze medewerkers. Via een piket- en-of bereikbaarheid dienst kan er in het geval van acute dreigingen en incidenten, ook buiten kantooruren een beroep op je worden gedaan.

Acquisitie naar aanleiding van deze vacature wordt niet op prijs gesteld.

## Meer over de functiegroep Coördinerend / Specialistisch Adviseur

Door het Functiegebouw Rijk worden medewerkers en leidinggevenden geholpen bij het maken van resultaat- en ontwikkelafspraken in functioneringsgesprekken en krijgt men inzicht in de loopbaanmogelijkheden binnen de Rijksoverheid.

[Meer informatie op Functiegebouw Rijksoverheid](#) 

---

## Nationaal Cyber Security Centrum

Het NCSC werkt aan een digitaal veilig Nederland. Door het tempo waarin het cybersecuritydomein zich ontwikkelt en de rol van het NCSC daarin, ligt er een flinke uitdaging voor de toekomst. Het is voor ons als hét kennisinstituut van cybersecurity in Nederland essentieel dat wij Nederland van kwalitatief hoogwaardige en actuele informatie voorzien, in crisistijd en daarbuiten. Deze kennis en kunde halen wij mede uit en delen wij ook weer met ons netwerk (overheden, bedrijfsleven en andere nationale en internationale partners). Op deze wijze proberen we tijdig in te springen op nieuw ontdekte kwetsbaarheden, aanvalscampagnes en ernstige ICT-verstoringen om deze te voorkomen en op te lossen. Als het toch misgaat beperken we op deze manier de impact.

## Stel gerust je vraag



Meer informatie over deze vacature

**Amber de Groot**

 [recruitment.ncsc@minjenv.nl](mailto:recruitment.ncsc@minjenv.nl)



## Meer informatie over de sollicitatieprocedure

**Jeroen Prinse**

✉ [jeroen.prinse@ncsc.nl](mailto:jeroen.prinse@ncsc.nl)