Functiebenaming	Chief Information Security Officer (CISO)
Plaats in de organisatie	De functionaris ontvangt hiërarchisch en functioneel leiding van de Raad van Bestuur van de organisatie. De functionaris voert de (deels toezichthoudende) taken onafhankelijk uit.

Doel van de functie

De CISO Definieert het informatiebeveiligingsbeleid, gebaseerd op een risicomanagement-benadering en rekening houdend met het informatiebeveiligingsdreigingsbeeld, trends en organisatiebehoefte. Richt de informatiebeveiligingsorganisatie in, bepaalt de daarvoor benodigde middelen en de inzet hiervan op concrete beveiligingsmaatregelen. Initieert en coördineert de implementatie van informatiebeveiliging voor de gehele organisatie en houdt daar toezicht op. Zorgt voor een geschikt niveau van informatiebeveiliging en informatiebeveiligingsgedrag in de organisatie, gebaseerd op de behoeften en de risicobereidheid van de organisatie. Wordt door interne en externe stakeholders beschouwd als de deskundige op het gebied van informatiebeveiliging.

Producten

De CISO is verantwoordelijk voor:

- Opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen
- Het inrichten van de informatiebeveiligingsorganisatie
- Het coördineren en adviseren bij afhandelen van beveiligingsincidenten
- Afstemming van informatiebeveiliging met andere beveiligingsdomeinen
- Het toezien op naleving van de eisen voor informatiebeveiliging
- Het bevorderen van het informatiebeveiligingsbewustzijn over de hele organisatie
- De voorbereiding op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's o.b.v. het Cybersecuritybeeld Nederland (CSBN)
- Het adviseren bij en begeleiden van informatierisicoanalyses
- Het uitvoeren van informatiebeveiligingsassessments

De CISO realiseert:

- Certificering NEN 7510
- Projectportfolio voor informatiebeveiliging
- Organisatiebrede informatiebeveiligingsactiviteiten en -projecten
- Monitoring van de relevante risico's voor de organisatie
- Monitoring van compliance met beleid en wet- en regelgeving
- Gecoördineerde reactie op ernstige informatiebeveiligings- of ICT- incidenten
- Organisatiebrede richtlijnen, standaarden, methoden en technieken voor informatie-beveiliging Opstellen van vacatures in overleg met management en directie.

De CISO draagt bij aan:

- Risicomanagementbeleid
- Informatiesysteem-governance
- Service Level Agreements
- Informatiebeveiligingsarchitectuur

Kerntaken

- Definieert het informatiebeveiligingsbeleid voor de organisatie
- Organiseert informatiebeveiliging en de daarvoor benodigde expertise

- Zorgt voor afstemming tussen informatiebeveiliging met andere beveiligingsdomeinen, waaronder privacybescherming, fysieke beveiliging en continuïteitsmanagement
- Zet een informatiebeveiligingscalamiteitenorganisatie op
- Coördineert de reactie op ernstige informatiebeveiligings- of ICT-incidenten
- Zorgt voor een projectportfolio voor informatiebeveiliging
- Initieert en coördineert organisatiebrede informatiebeveiligingsactiviteiten en -projecten
- Zorgt voor organisatiebrede richtlijnen, standaarden, methoden en technieken voor informatiebeveiliging
- Monitort en borgt de kwaliteit van informatierisicoanalyses, beveiligingsontwerpen en oplossingen
- Monitort en borgt het naleven van de eisen en architectuur voor informatiebeveiliging en het consequent toepassen van Security-by-Design en Privacy-by-Design
- Monitort en borgt informatiebeveiligingsbewustzijn binnen de organisatie
- Monitort de relevante risico's voor de organisatie
- Borgt dat de organisatie voldoende voorbereid is op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's
- Monitort en borgt de kwaliteit van informatiebeveiligingsassessments
- Monitort op basis van assessments, test, reviews en audits in hoeverre de organisatie compliant is met het informatiebeveiligingsbeleid en wet- en regelgeving
- Informeert bestuur en management over de status van informatiebeveiliging en incidenten en presenteert verbetervoorstellen

Vereiste kennis

- Academisch werk en denkniveau.
- Kennis van relevante en toekomstige wet- en regelgeving omtrent de bescherming van persoonsgegevens.
- Kennis van governance en compliance.
- Kennis van informatie- en communicatietechnologie.
- Kennis van informatiebeveiliging.
- Kennis van de administratieve organisatie.
- Kennis van Privacy Impact Assessment (PIA).
- Kennis van audits.
- Kennis van integriteit en ethiek op het gebied van privacyvraagstukken.
- Heeft kennis van doel, (juridische en organisatie) structuur, beleid en wijze van functioneren van de organisaties.
- Vakkennis dient op peil te worden gehouden, bijvoorbeeld door het lezen van vakliteratuur, het volgen van specifieke bij- en nascholing en cursussen en het bezoeken van studiedagen of symposia op het vakgebied.

Zelfstandigheid

- Werkt zeer zelfstandig aan de hand van NEN- en CISO-normeringen waarbij afgewogen keuzes moeten worden gemaakt en waarbij de werkwijze naar eigen inzicht wordt bepaald.
- Vertaalt de problematiek en wet- en regelgeving in correcte procedures, adviezen en overige documenten. Is hierbij in staat om zowel zelfstandig als in teamverband te werken.

Sociale vaardigheden

- Bij het geven van advies, het verstrekken van informatie en het behandelen c.q. beoordelen van beveiligingsincidenten/datalekken worden hoge eisen gesteld aan tact, luistervaardigheid, gespreksvoering, probleemoplossend vermogen, het omgaan met

tegenstellingen en het kunnen overtuigen.

Risico's, verantwoordelijkheid en invloed

- Er is sprake van professionele verantwoordelijkheid bij het uitbrengen van adviezen en het verstrekken van informatie, het interpreteren en toepassen van wet- en regelgeving en het behandelen c.q. beoordelen van beveiligingsincidenten.
- Er bestaat kans op materiële en immateriële schade bij het geven van onjuiste of onvolledige informatie en adviezen. Bij de diverse in- en externe contacten kan de goede naam van de organisaties nadelig worden beïnvloed.

Uitdrukkingsvaardigheid

- Hoge eisen worden gesteld aan de mondelinge uitdrukkingsvaardigheden bij in- en externe contacten.
- Zeer hoge eisen worden gesteld aan schriftelijke uitdrukkingsvaardigheden. De correcte terminologie dient te worden gehanteerd bij het opstellen van de diverse documenten.
- Beschikt verder over het vermogen om ideeën en opvattingen helder en beknopt schriftelijk te verwoorden en gevoelige onderwerpen diplomatiek te beschrijven.

Bewegingsvaardigheid

- Er worden geen bijzondere eisen aan de bewegingsvaardigheid gesteld. Bij de uitvoering van de werkzaamheden wordt veelvuldig gebruik gemaakt van de computer.

Oplettendheid

- Oplettendheid is nodig bij de adviserende, begeleidende en uitvoerende werkzaamheden en het beoordelen en behandelen van beveiligingsincidenten, waarbij in ruime mate aandacht is vereist voor zowel grote lijnen als details en de belangen van de organisaties.

Overige functie-eisen

- Beschikt over volharding en een groot doorzettingsvermogen teneinde de nodige informatie te vergaren om een volledig advies dan wel informatie te verstrekken alsmede om een beveiligingsincident op juiste wijze te kunnen beoordelen.
- Systematiek en ordelijkheid is vereist bij de analyse van het vraagstuk op grond waarvan een advies en informatie wordt geformuleerd.
- Hoge eisen worden gesteld aan het kunnen omgaan met gevoelige informatie, integriteit en betrouwbaarheid.
- Eisen worden gesteld aan voorkomen en gedrag in verband met het onderhouden van in- en externe contacten binnen het werkveld.
- Aanzienlijke objectiviteit is vereist.

Inconveniënten

- Psychische belasting kan optreden door cumulaties van verantwoordelijke werkzaamheden onder tijdsdruk.
- Tevens kan psychische belasting plaatsvinden doordat men te maken krijgt met conflicterende belangen die kunnen optreden tussen individuele medewerkers en de organisatie, tussen verschillende organisatieonderdelen of in externe samenwerkingsrelaties.

Salaris

Inschaling vindt plaats in schaal 65 van de cao ziekenhuizen.