Functiebeschrijving ICT beheer en SO

Afdeling

ICT & Informatiebeveiliging

Rapporteert aan

Directie

Doel van de functie

De ICT Beheerder & Security Officer is verantwoordelijk voor het beheer en de beveiliging van de on-premise ICT-infrastructuur, de interne Azure Cloud-omgeving van de organisatie en de Azure Cloud-omgevingen van klanten. Daarnaast waarborgt deze functionaris de naleving van informatiebeveiligings- en privacybeleid, conform ISO 27001:2022 en relevante wet- en regelgeving.

Kernverantwoordelijkheden

1. ICT Beheer

- Beheer en onderhoud van de on-premise ICT-infrastructuur, inclusief servers, netwerken en werkplekken.
- Configuratie, monitoring en onderhoud van de interne Azure Cloud-omgeving.
- Ondersteunen en beheren van Azure Cloud-omgevingen van klanten.
- Implementeren van back-up- en recoverystrategieën voor zowel on-premise als cloudomgevingen.
- Toepassen van principes voor secure architecture en secure development.
- Proactief signaleren, analyseren en oplossen van technische problemen en storingen.

2. Security & Privacy

- Beheer en implementatie van beveiligingsmaatregelen binnen de ICT-omgeving en cloudomgevingen.
- Identificeren en beheren van risico’s door middel van risicoanalyses en vulnerability assessments.
- Coördineren en implementeren van security policies, procedures en controles conform ISO 27001:2022.
- Zorgdragen voor de naleving van AVG/GDPR en andere relevante regelgeving.
- Beheer en uitvoering van dataclassificatie, incidentbeheer en forensisch onderzoek bij beveiligingsincidenten.
- Organiseren en uitvoeren van beveiligingsbewustzijnstrainingen binnen de organisatie.

3. Audit & Compliance

- Opstellen en beheren van documentatie en rapportages ten behoeve van audits en certificeringstrajecten.
- Begeleiden van interne en externe audits en uitvoeren van interne controles.
- Adviseren van de directie over beveiligingsmaatregelen, risico’s en verbeterinitiatieven.
- Zorgdragen voor de opvolging van auditbevindingen en het continue verbeteren van beveiligingsmaatregelen.

4. Cinnovate technologie

- Beheer Cinnovate software en klant configuraties.
  - UpdateServer
  - CareServer
  - Devices: Assist App, Icoms, Multi Controllers, etc.
- Implementatie en configuratie van Cinnovate systemen, zowel op locatie als op afstand.
- Service en support binnen en buiten kantooruren aan Cinnovate klanten.

Competenties & Vaardigheden

- Diepgaande kennis van Microsoft Azure en cloudbeheer.
- Ervaring met het beheer van on-premise ICT-infrastructuur.
- Kennis van en ervaring met ISO 27001:2022, NEN 7510 en AVG/GDPR.
- Vaardigheid in het uitvoeren van risicoanalyses en implementeren van beveiligingsmaatregelen.
- Probleemoplossend en analytisch vermogen.
- Sterke communicatieve vaardigheden en vermogen om security awareness te verhogen binnen de organisatie.
- Vermogen om te schakelen tussen operationeel beheer en strategische security-initiatieven.

Opleiding & Ervaring

- Minimaal een afgeronde hbo-opleiding in ICT, Cybersecurity of een vergelijkbare richting.
- Minimaal 5 jaar relevante werkervaring in ICT-beheer en informatiebeveiliging.
- Certificeringen zoals Microsoft Azure Administrator (AZ-104), CISSP, CISM of ISO 27001 Lead Implementer zijn een pré.

Arbeidsvoorwaarden

- Fulltime functie (32-40 uur per week).
- Flexibele werktijden en mogelijkheid tot hybride werken.
- Opleidings- en certificeringsmogelijkheden in zowel ICT-beheer als security.

Samenvatting

De ICT Beheerder & Security Officer speelt een cruciale rol in zowel het technisch beheer als de beveiliging van de ICT-omgeving binnen de organisatie en bij klanten. Met een brede verantwoordelijkheid in zowel operationeel als strategisch beheer, draagt deze functionaris bij aan de continuïteit, beveiliging en naleving van wet- en regelgeving binnen het ICT-landschap.