|  |
| --- |
| **FUNCTIEBESCHRIJVING**  **Information Security Officer (ISO) – Senior** |

# CONTEXT VAN DE FUNCTIE BINNEN DE ORGANISATIE

De Vlaamse ICT-vereniging is een kosten- en kennis-delende organisatie, die strategische ICT-brugfuncties ter beschikking stelt van haar leden-overheidsorganisaties. Dit met het doel om deze leden te ondersteunen bij het realiseren van het ICT-beleid en bij het afstemmen van het ICT-beleid op de noden en doelstellingen van de overheidsorganisatie. De vereniging richt zich dan ook specifiek op ICT-expertise die cruciaal is om een brug te slaan tussen de bedrijfsvoering enerzijds en ICT anderzijds.

Het is in deze context dat de functie zal ingeschakeld worden binnen de leden van de Vlaamse ICT-vereniging. Daarbij wordt een hoge mate van strategisch en klantgericht denken gehanteerd, waarbij de functie essentieel deel zal uitmaken van de organisatie in een duurzaam partnership op (middel)lange termijn.

# DOEL VAN DE FUNCTIE

Je bent verantwoordelijk voor het verzekeren en controleren van de informatieveiligheid teneinde de vertrouwelijkheid (confidentiality), de beschikbaarheid (availability), de integriteit (integrity), de onbetwistbaarheid (non repudiation) en de toerekenbaarheid (accountability) van de gegevens te verzekeren.

Je levert een bijdrage aan de ontwikkeling van het Informatiebeveiligingsbeleid. Je adviseert over technische uitdagingen en zorgt ervoor dat de ontwikkeling, communicatie en onderhoud van standaarden, procedures en andere documentatie die het beveiligingsbeleid ondersteunen. Je ondersteunt beveiligingsprojecten en zorgt ervoor dat ze met succes worden uitgevoerd.

Deze functie heeft een rol bij enerzijds de ontwikkeling van nieuwe projecten/systemen, en anderzijds het onderhoud en beheer van bestaande systemen, applicaties en infrastructuur.

# AANSTURING

|  |  |  |
| --- | --- | --- |
| Rapporteert hiërarchisch aan | Teamcoach |  |
| Rapporteert functioneel aan | CISO  Kenniscoördinator |  |
| Stuurt hiërarchisch aan |  |  |
| Stuurt functioneel aan |  |  |

# DIMENSIES VAN DE FUNCTIE

Omschrijving van de opdracht:

Als Information Security Officer (ISO) implementeer je de informatiebeveiliging in overeenstemming met de informatiebeveiligingsstrategie van de organisatie.

Belangrijkste verantwoordelijkheden:

 Je ondersteunt de ontwikkeling van een strategisch veiligheidsbeleid, zowel op korte als lange termijn, en implementeert informatiebeveiliging in de organisatie.

 Je implementeert de vertaling naar informatiebeveiligingsplannen voor programma's, projecten en exploitaties. Je werkt nauw samen met andere ISOs en security architecten in de projecten en programma's en met de DPO.

 Je vertaalt de informatiebeveiligingsbehoefte van de organisatie naar beveiligingsmaatregelen.

 Je zorgt in het kader van informatiebeveiliging voor een beveiligingsplan, risicoanalyses, risicomonitoring, incidentenregistratie, hulpmiddelen, training and evaluatie.

 Je initieert en coördineert de opmaak van risicoanalyses, het opzetten, monitoren van registraties op vlak van beveilingsmaatregelen.

 Je controleert de naleving van het controleplan en geeft ondersteuning bij het uitvoeren daarvan, je initieert interne audits.

 Je monitort informatiebeveiligingsrisico’s en rapporteert daarover

 Je initieert en bestuurt informatiebeveiliging- en bewustwordingsprojecten.

 Je wordt door interne en externe stakeholders beschouwd als de deskundige op het gebied van informatiebeveiliging.

 Je neemt initiatief om de werking binnen het vakgebied informatiebeveiliging te optimaliseren, neemt hierbij een trekkende rol op. Je voorziet in een gedocumenteerde kennisverzameling voor informatiebeveiliging

 Je zorgt voor training en opleiding voor informatiebeveiligingsbewustzijn

 Je treedt op als projectmanager bij beveiligingsprojecten, waarbij aansturing wordt gegeven aan projectleiders binnen de programma's.

# RESULTAATGEBIEDEN

|  |  |
| --- | --- |
| 1. Behoefteanalyse | * Ondersteunt de opmaak en verdediging van business cases rond informatiebeveiliging, het beheer en de opvolging van de doelstellingen. * Vertaalt de informatiebeveiligingsbehoefte van de organisatie naar beveiligingsmaatregelen |
| 2. Dienstverlening uitbouwen | * Ondersteunt de ontwikkeling van een actueel informatiebeveiligingsbeleid (langere termijn) en standaarden voor eigen entiteit en afdelingen. * Implementeert informatiebeveiliging in de organisatie * Coördineert de vertaling van het informatieveiligheidsbeleid naar informatiebeveiligingsplannen voor programma's, projecten, exploitaties. * Houdt toezicht op de implementatie en naleving van het informatiebeveiligingsbeleid. * Stemt informatiebeveiligingsactiviteiten en -projecten af met andere beveiligingsdomeinen, waaronder privacybescherming en fysieke beveiliging. * Initieert en coördineert de opmaak van risicoanalyses, het opzetten, monitoren van registraties op vlak van beveilingsmaatregelen. * Ondersteunt de ontwikkeling van een controleplan een de uitvoering daarvan. * Zet een informatiebeveiligingscalamiteiten-organisatie op * Coördineert de reactie op ernstige informatiebeveiligings- of ICT-incidenten * Draagt zorg voor het registreren van beveiligingsincidenten evenals het afhandelen van opgetreden incidenten en het nemen van preventieve maatregelen. * Voorziet in een gedocumenteerde kennisverzameling voor informatiebeveiliging * Zorgt voor informatiebeveiligingsontwerpen en -oplossingen en de implementatie van security-by-design en privacy-by-design in informatiesystemen * Draagt bij aan organisatiebrede richtlijnen, standaarden, methoden en technieken voor informatiebeveiliging |
| 3. Optimalisatie van de werking/dienstverlening | * Neemt initiatief om de werking binnen het vakgebied informatiebeveiliging te optimaliseren, neemt hierbij een trekkende rol op. * Presenteert verbetervoorstellen aan het management met betrekking tot informatiebeveiliging en -risico’s |
| 5. Werkinstrumenten | * Bedenkt, bouwt en onderhoudt tools en werkinstrumenten die efficiënt, effectief zijn ter ondersteuning van de werking. * Waakt erover of de tools optimaal worden ingezet en of ze de behoeften voldoende blijven invullen, stuurt bij waar nodig. * Zorgt voor de ontwikkeling van een Projectportfolio voor informatiebeveiliging * Stelt instructies en procedures op en leeft ze na, zodat systeemveiligheid op een uniforme manier doorheen eigen entiteit verloopt. |
| 6. Adviesverlening | * Geeft gevraagd en ongevraagd advies aan programmamanagers en directieleden ten aanzien van informatiebeveiliging. * Ondersteunt de rapportage aan de directie over het gevoerde beleid met betrekking tot informatiebeveiliging, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, ondernomen acties, resultaten van onderzoeken en resultaten van controles. |
| 7. Kwaliteitsborging | * Is verantwoordelijk voor het opzetten van bewaking van de informatiebeveiliging. * Voorziet in duidelijke en tijdige rapportages die inzicht geven aan het management wat het niveau van informatiebeveiliging is, hoe de risico's beperkt worden in verhouding tot het risicoprofiel en welke de voorvallen zijn betreffende cybersecurity. * Volgt de doelstellingen voor informatiebeveiliging nauw op. * Monitort informatiebeveiligingsrisico’s en rapporteert daarover * Realiseert en monitort informatiebeveiligings-assessments, -tests, -reviews en -audits |
| 8. Communicatie en contacten | * Zorgt voor de sensibilisatie en de naleving van de veiligheidsregels en de regels betreffende de informatie en informatiesystemen aan. * Zorgt voor training, opleiding en kennisuitwisseling op het gebied van informatiebeveiligingsbewustzijn * Ondersteunt de ontwikkeling van het communicatieplan op en zorgt voor de uitvoering ervan. * Onderhoudt interne en externe contacten op alle niveaus binnen de expertise van systeemveiligheid. |
| 9. Kennis m.b.t. het vakgebied | * Is een specialist voor het expertisedomein binnen eigen entiteit * Neemt pro-actief een actieve positie in bij Vlaamse overheidsinitiatieven en projecten. * Bouwt de kennis verder uit en verankert deze binnen de organisatie met als doel het kennisniveau op peil te houden. |
| 10. Projectdeelname | * Treedt op als projectmanager bij beveiligingsprojecten, waarbij aansturing wordt gegeven aan projectleiders binnen de prgramma's/projecten. * Initieert nieuwe informatiebeveiligingsprojecten in lijn met het informatieveiligheidsbeleid. * Ondersteunt organisatiebrede informatiebeveiligingsprojecten en -programma's |
| 11. Beleidsvoorbereiding | * Zorgt voor het uitwerken en uitrollen van het beleid voor informatiebeveiliging, zowel op korte als op lange termijn. Het beleid past binnen de krijtlijnen van de strategie van eigen entiteit. * Neemt een adviserende rol op voor de strategie van eigen entiteit in het algemeen, met aandacht alle relaties van het eigen expertisedomein met ander expertisedomeinen. * Presenteert informatiebeveiligingsoplossingen aan collega’s en leidinggevenden |
| 12. Organisatie - en samenwerkingsvorm | * Bouwt de kennis verder uit en verankert binnen de organisatie met als doel het kennisniveau op peil te houden. * Stuurt collega's vakinhoudelijk aan de uitvoering van dagelijkse operationele activiteiten. |

# CONTACTEN

* **INTERNE CONTACTEN**

Uitwisselen van informatie : Leidend Ambtenaar, CISO, andere ISOs, DPO, hoofd ICT, hoofd fysieke beveiliging, HR, Bureau Informatiebeveiliging en Gegevensbescherming

Onderhandelen met :

* **EXTERNE CONTACTEN**

Uitwisselen van informatie : CISO en teamleden Team Informatieveiligheid Vlaamse Overheid, andere ISOs, Werkgroep Informatieveiligheid, dienstenleveranciers

Onderhandelen met :

# FUNCTIONERINGSCRITERIA

1. Gewenst minimaal opleidingsniveau:
2. Zeer goede kennis van het Nederlands is noodzakelijk, alsook een goede kennis van het Engels.
3. Ervaring en inwerkperiode

|  |  |  |  |
| --- | --- | --- | --- |
| Vereiste ervaring (in een gelijkaardige functie/vakdomein waarvan x in een relevante sector) + inwerkperiode (periode nodig om op zelfstandige wijze de functie te kunnen uitvoeren) | | | |
|  | In een gelijkaardige functie | In een relevante sector | Inwerkperiode |
| < 3 maanden |  |  |  |
| 3 m – 1j |  |  |  |
| 1j – 4j |  | X |  |
| 4j – 7j | X |  | 2 maanden |
| >7 jaar |  |  |  |

1. Vaktechnische competenties :

Aantoonbare kennis/ervaring:

* Minimum 5 jaar ervaring als teamlid in securityprojecten
* Minimum 3 jaar – ideaal 5 jaar ervaring op het vlak van architecturale conceptuele vaardigheid
* Minimum 3 jaar ervaring met het hanteren datamodelling en development methodieken
* Minimum 3 jaar – ideaal 5 jaar ervaring met het opzetten en implementeren van architectuurstrategieën

Pluspunt:

* Ervaring met stakeholder engagement in de publieke sector.
* Ervaring in de rol van security analist en het afhandelen van security incidenten
* Ervaring in de rol van security architect
* Ervaring met Agile aanpak en mindset
* Ervaring met het opzetten en uitvoeren van penetratietesten
* Ervaring met het aanreiken van optimalisatievoorstellen vanuit incidenten

1. Gedragscompetenties

|  |  |
| --- | --- |
| **verantwoordelijkheid nemen**  Handelen in overeenstemming met de belangen, waarden en normen van de organisatie | Niveau 2 - Handelt in het belang van de organisatie  • Draagt actief bij aan de doelen en waarden van de organisatie  • Overweegt de gevolgen van zijn voorstellen en acties voor de organisatie  • Blijft consequent handelen, ook in lastige of onzekere situaties  • Zegt wat hij doet, is open over de door hem gehanteerde waarden en normen  • Wekt vertrouwen in zijn objectiviteit en integriteit |
| **Samenwerken**  Een bijdrage leveren aan een gezamenlijk resultaat in een team of project, ook als dat niet meteen van persoonlijk belang is | Niveau 2 - Stimuleert de samenwerking binnen zijn entiteit, werkgroepen of projectgroepen  • Laat het gemeenschappelijk belang van de organisatie primeren op het persoonlijk belang  • Komt met ideeën om het gezamenlijke resultaat te verbeteren  • Betrekt belanghebbenden bij het nemen van beslissingen, stemt consequenties van acties en beslissingen met betrokkenen af  • Moedigt anderen aan om van gedachten te wisselen, te overleggen en samen opdrachten aan te pakken  • Onderneemt acties zodat er een positieve verstandhouding en productieve samenwerking binnen de groep ontstaat en blijft |
| **Klantgerichtheid**  Wensen en behoeften van de verschillende belanghebbenden binnen en buiten de organisatie onderkennen en er adequaat op reageren | Niveau 2 - Optimaliseert de dienstverlening aan belanghebbenden binnen afgesproken kaders  • Onderzoekt de wensen, behoeften en verwachtingen van belanghebbenden via gericht systematisch onderzoek (tevredenheidsenquêtes, mondelinge enquêtes, …)  • Verleent nazorg en onderneemt concrete acties naar aanleiding van specifieke feedback van belanghebbenden  • Gaat kritisch na op welke punten de dienstverlening kan worden verbeterd en formuleert hiertoe concrete voorstellen  • Zet nieuwe mogelijkheden op het vlak van dienstverlening meteen om in de praktijk  • Onderneemt acties om de dienstverlening aan specifieke doelgroepen te optimaliseren, rekening houdend met hun beperkingen en behoeften (bv. handicap, kinderen, …) |
| **Analyseren**  Een probleem duiden in zijn verbanden en op een efficiënte wijze op zoek gaan naar aanvullende relevante informatie. | Niveau 3 - Maakt verhelderende analyses van complexe vraagstukken  • Herformuleert complexe vraagstukken naar hanteerbare vragen  • Plaatst het vraagstuk of probleem in een breder kader  • Houdt bij de analyse rekening met verschillende aanknopingspunten  • Ziet trends en patronen in ogenschijnlijk niet-gerelateerde feiten  • Betrekt en integreert tegengestelde oordelen in zijn analyse |
| **Oordeelsvorming**  Mening uiten en zicht hebben op de consequenties ervan, op basis van een afweging van relevante criteria | Niveau 3 - Vormt een geintegreerd oordeel  • Heeft een veelzijdige, genuanceerde kijk  • Neemt in zijn standpunt verschillende belangen in overweging  • Benoemt zowel de positieve als negatieve kanten van zijn standpunt of voorstel  • Heeft oog voor kritieke factoren en activiteiten en benut de mogelijkheden hiervan voor de organisatie  • Vertaalt een synthese naar een vraagstelling of advies en geeft zo een inhoudelijke meerwaarde aan de thema's die hij naar voren brengt |
| **Initiatief**  Kansen onderkennen en uit eigen beweging acties voorstellen of ondernemen | Niveau 3 – Neemt initiatieven om op gebeurtenissen en ontwikkelingen te anticiperen (proactief)  • Signaleert kansen en onderneemt hier actie op  • Introduceert verbeteringen in werkaanpak en procedures  • Anticipeert middels actie op diverse situaties  • Zoekt actief naar kansrijke ontwikkelingen voor de organisatie en pakt deze op  • Zorgt voor een werkklimaat waarbinnen voldoende autonomie bestaat om initiatieven te nemen |
| **Resultaatgerichtheid**  Concrete en gerichte acties ondernemen om doelstellingen te behalen of te overstijgen | Niveau 2 – Formuleert uitdagende (maar haalbare) doelstellingen en zet zich ten volle in om die te bereiken  • Legt de lat hoog, formuleert uitdagende (maar haalbare) doelstellingen  • Gaat actief op zoek naar de best mogelijke manier om doelen te bereiken, weegt opties tegen elkaar af  • Mobiliseert mensen en middelen, ook als hij hiertoe anderen (hiërarchie, collega’s) moet overtuigen  • Evalueert op regelmatige basis zijn resultaten en stuurt het proces bij om de doelstellingen te behalen  • Geeft niet op, zoekt actief naar alternatieven als hij met hindernissen en tegenslagen te maken krijgt |
| **Communiceren**  Informatie en ideeën schriftelijk en/of mondeling begrijpelijk overbrengen | Niveau 3 – Communiceert vlot met verschillende doelgroepen, ook over complexe onderwerpen  • Geeft abstracte of complexe materie op een inzichtelijke wijze weer  • Bouwt zijn betoog op een gericht gestructureerde wijze op  • Communiceert selectief vanuit zijn inzicht in de situatie, om zo sneller zijn doel te bereiken  • Zoekt aansluiting bij het publiek en gebruikt voor hen relevante en overtuigende redeneringen, argumenten, voorbeelden en vergelijkingen  • Hanteert een rijk en gevarieerd taalgebruik  • Kiest een communicatiewijze naargelang de behoeften, mogelijkheden of eigenheden van het doelpubliek  • Hanteert een stijl die aangepast is aan de situatie (zakelijk, onderhoudend, informatief, interactief, …)  • Richt zich tot het publiek en neemt het in zijn gedachtegang mee  • Zorgt voor een correcte uitwisseling van informatie (gaat na of zijn boodschap duidelijk is, vat de boodschap van anderen samen, …)  • Stimuleert de communicatie in twee richtingen (stelt vragen, verzoekt om inbreng, …) |
| **Visie**  Feiten in een ruime context plaatsen en een toekomstgericht beleid ontwikkelen | Niveau 2 – Betrekt brede (maatschappelijke, technische …) factoren bij zijn aanpak  • Plaatst adviezen, beslissingen en initiatieven in de brede organisatiecontext of beleidscontext  • Kent de relevante trends en ontwikkelingen binnen zijn beroep of domein  • Wijst op evoluties die voor anderen nog onbekend zijn  • Heeft voeling met wat er in de toekomst gevraagd kan worden  • Levert een bijdrage aan het ontwikkelen van het beleid voor zijn werkveld |