FUNCTIEBESCHRIJVING
Chief Information Security Officer (CISO)

1. CONTEXT VAN DE FUNCTIE BINNEN DE ORGANISATIE

De Vlaamse ICT-vereniging is een kosten- en kennisdelende 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.

Hierbij wordt een hoge wendbaarheid gehanteerd, waarbij de ter beschikking gestelde profielen kunnen doorstromen tussen de verschillende leden van de vereniging. Een aanbeveling die hierbij gehanteerd wordt is een doorstroming van de functie binnen een termijn van maximum 4 jaar naar andere overheidsorganisaties en meewerken aan projecten waar meerdere beleidsdomeinen en leden bij betrokken zijn.

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.

2. DOEL VAN DE FUNCTIE

De Chief Information Security Officer (verder CISO) staat in voor het verzekeren en controleren van de informatiebeveiligingsbeleid teneinde de vertrouwelijkheid (confidentiality), de beschikbaarheid (availability), de integriteit (integrity), de onbetwistbaarheid (non repudiation) en de toerekenbaarheid (accountability) van de gegevens te verzekeren. Deze persoon is verantwoordelijk voor de ontwikkeling en uitvoering van de I&T veiligheidsstrategie voor heel de organisatie:

- Volledige accountability en verantwoording voor de veiligheid van alle informatie en toegangscontrole binnen de organisatie. Dit omhelst het bepalen van een veiligheidsstrategie mbt de klanten van de organisatie (4 miljoen burgers, duizenden werkgevers en partners) en dit in een context waarbij de organisatie data uitwisselt met externe partijen binnen en buiten de eigen organisatie.
- Uitstippelen en uitvoeren van de Informatie veiligheidsstrategie en -raamwerk voor heel de organisatie zodat de operaties schaalbaar en veilig verlopen. Bepalen van I&T en business actiestappen en het laten naleven door strakke governance en rapportering en desnoods corrigerende maatregelen
- Het opstellen van de technische I&T veiligheidsprojectenroadmap via meerjarenplanning zodat de organisatie I&T en business veiligheid minstens 4 behaalt en behoudt op Gartner benchmarkings
- Veto- en beslissingsrecht mbt business veiligheidsvraagstukken; draagvlak creëren bij alle stakeholders, zowel interne als externe
- Driemaandelijkse rapportering aan het directiecomité mbt stand van zaken van de informatieveiligheid in de organisatie
- Aanspreekpunt bij veiligheidsaudits van Federale en Vlaamse entiteiten
- Verantwoordelijk voor behalen en houden van security ISO normen en het definiëren van de nodige projecten en maatregelen desgevallend
- Coördineren en adviseren bij beveiligingsincidenten en zo nodig optreden bij calamiteiten.
- Te allen tijde een open deur dienen te hebben voor de gebruikersorganisatie indien deze, buiten de hiërarchie om, een beveiligingsincident wil melden.
- Formeel aanspreekpunt en single point of escalatie voor alle informatiebeveiligingszaken.

- Leiden van het I&T crisismanagement team en ondersteuning van de algemene directie in geval van calamiteiten.
- Bepalen van de disaster recovery strategie en opvolging van de uitrol en testen binnen de Operations afdeling.
- Bepalen van de strategie om het bewustzijn binnen DE ORGANISATIE van alle medewerkers mbt informatie veiligheid te verhogen en mitigerende maatregelen te bepalen. Opzetten en initiëren van (periodieke) bewustzijnprogramma's (o.a. regelmatige phishing campagnes, friendly hackings, …) en adviseren mbt voorlichting en training van gebruikers in het correct omgaan met informatie(systemen).
- Verlenen van technische adviezen in de I&T openbare aanbestedingen

3. AANSTURING

Rapporteert hiërarchisch aan	CIO	
Rapporteert functioneel aan		
Stuurt hiërarchisch aan	Security engineers Security architect Security PM Security admin Security Operations Center	5-15 medewerkers
Stuurt functioneel aan		Niet van toepassing < 5 medewerkers 5-15 medewerkers +15 medewerkers

4. DIMENSIES VAN DE FUNCTIE

- Situeert zich op strategisch niveau binnen de organisatie en rapporteert in die zin rechtstreeks aan de CIO
- Is een autoriteit voor het expertisedomein
- Volledige accountability en verantwoording voor de veiligheid van alle informatie en toegangscontrole binnen de organisatie. Dit omhelst het bepalen van een veiligheidsstrategie mbt de klanten van de organisatie (4 miljoen burgers, duizenden werkgevers en partners) en dit in een context waarbij de organisatie data uitwisselt met externe partijen binnen en buiten de organisatie.
- Treedt, wat de IT-veiligheid betreft, op als tussenpersoon voor alle contacten buiten de organisatie. Dit zijn contacten op C-level.

AUTONOME BESLISSINGSBEVOEGDHEID

- Werkt op zeer autonome basis met de andere functies die actief zijn in en/of belang hebben bij informatiebeveiling
- Moet zeer proactief te werk gaan en zelf de nodige stappen en initiatieven hiertoe nemen
- **Veto- en beslissingsrecht** mbt business veiligheidsvraagstukken; draagvlak creëren bij alle stakeholders, zowel interne als externe

5. RESULTAATGEBIEDEN

RESULTAATGEBIED 1 : informatiebeveiligingsbeleid

Doel : uitwerken & implementeren van het beleid inzake informatiebeveiliging

Deelactiviteiten :

- ✓ formuleert tactisch-strategisch advies op vlak van informatiebeveiliging.
- ✓ Coördineert de vertaling van het informatieveiligheidsbeleid naar informatiebeveiligingsplannen voor programma's, projecten, exploitaties
- ✓ Neemt het voortouw in de aanneming, goedkeuring en het onderhoud van het Information Security Framework, coördinatie en follow-up van diverse projecten en initiatieven binnen de informatiebeveiliging afdeling
- ✓ Houdt toezicht op de implementatie en naleving van het informatiebeveiligingsbeleid.
- ✓ Neemt initiatief om de werking binnen het vakgebied informatiebeveiliging te optimaliseren, neemt hierbij een trekkende rol op.
- ✓ Is verantwoordelijk voor doorlopend toezicht op de directie, de medewerkers, het beleid, de bedrijfsprocessen, de uitvoering en de apparatuur van de organisatie wat beteft informatiebeveiliging
- ✓ Rapporteert 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

RESULTAATGEBIED 2 : Uitbouwen dienstverlening

Doel : Continue opvolging van de (operationele) dienstverlening op vlak van informatieveiligheid.

Deelactiviteiten :

- ✓ Capteert behoeften op vlak van informatieveiligheid vanuit een gestructureerde analyse.
- ✓ Coördineert bedenken, bouwen en onderhouden van 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.
- ✓ Stelt instructies en procedures op en leeft ze na, zodat systeemveiligheid op een uniforme manier verloopt binnen de organisatie
- ✓ Is verantwoordelijk voor het opzetten van bewaking van de informatiebeveiliging.
- ✓ Houdt toezicht op de implementatie en naleving van procedures inzake informatieveiligheid.
- ✓ Geeft gevraagd en ongevraagd advies aan programmamanagers en directieleden ten aanzien van 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.
- ✓ Initieert interne audits.
- ✓ Volgt het toegewezen budget nauw op.

RESULTAATGEBIED 3 : People management

Doel : Aansturen, ontwikkelen en evalueren van medewerkers, teneinde steeds over competente en gemotiveerde medewerkers te beschikken.

Deelactiviteiten :

- ✓ Managen en motiveren van de medewerkers in het team.
- ✓ In overleg en samenwerking met de HR-/personeelsverantwoordelijken, instaan voor een geïntegreerd en efficiënt HR-beleid binnen de eigen afdeling

- ✓ (Bijdragen tot het) aantrekken ("branding"), selecteren, rekruteren en onthalen van de geschikte medewerkers
- ✓ Inzetten van medewerkers in processen & projecten conform competenties, talenten en ambities
- ✓ Talenten en ontwikkelingsmogelijkheden van medewerkers identificeren, instaan voor de vorming en competentie-ontwikkeling van medewerkers, interne mobiliteit en loopbaanontwikkeling stimuleren
- ✓ Verzekeren van een goede uitvoering van het prestatiemanagementproces (afspreken van doelstellingen, opvolgen, coachen en begeleiden, evalueren en waarderen)
- ✓ Integer toepassen van het beloningsbeleid

RESULTAATGEBIED 4 : Kennisoverdracht

Doel : Waarborgen van kennis, expertise en ervaring omtrent Informatiebeveiliging binnen de organisatie .

Deelactiviteiten :

- ✓ Bouwt de kennis verder uit en verankert deze binnen de organisatie met als doel het kennisniveau binnen de organisatie op vereiste peil te brengen/houden.
- ✓ Coördineert alle initiatieven (vb: voorlichting en interne opleidingen) van het personeel op het gebied van informatiebeveiliging.

Indien de werking van het team of de organisatie als geheel het vereist, kunnen er in overleg tijdelijk bijkomende verantwoordelijkheden toegekend worden.

6. CONTACTEN

- **INTERNE CONTACTEN**

Uitwisselen van informatie : Directie, Leidinggevende niveaus in de organisatie, alle medewerkers.

Onderhandelen met : Directie en Business verantwoordelijken/managementleden

- **EXTERNE CONTACTEN**

Uitwisselen van informatie : Breed professioneel netwerk , Magda, KSZ, VO, …

Onderhandelen met : Leveranciers van producten of diensten inzake informatiebeveiliging

7. FUNCTIONERINGSCRITERIA

1. Gewenst minimaal opleidingsniveau (niet vereist) :

   Master, bij voorkeur in een ICT-gerelateerde richting, of gelijkwaardig door specifieke ervaring in persoonsgegevensbescherming en/of informatiebeveiliging.

2. 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			X
1j – 4j			
4j – 7j			
>7 jaar	X		

3. Vaktechnische competenties :

Vaktechnisch ICT competentiedomein *(Dit zijn domeinen waarbinnen vaktechnische competenties zich situeren, eerder dan specifieke competenties. Hierbij is ook geen definitie, noch niveaubepaling. Het is eerder een overzichtelijke aanduiding in welke richting de vaktechnische competenties zich moeten situeren. Het focust enkel op deze domeinen die onontbeerlijk zijn binnen de functie, niet op alle domeinen die nuttig zouden kunnen zijn.)*	
Business intelligence & data management	
IT Strategy and Planning	
Business Process Analysis	
Business Process Improvement	
Security and Risk Management	
Program and Project Management	
Architecture Management	
Business Relationship Management	
Service Delivery Management	
Infrastructure and Operations	
Customer Service (Help Desk)	
Application Development and Management	
Sourcing management	
Vendor management	
ICT Human Resources	
ICT Finance	

4. 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

Inleving

Alert zijn op gevoelens en behoeften van anderen en daar adequaat op reageren

Niveau 3 – Speelt in op complexe wensen en behoeften

- Speelt gepast in op impliciete en onuitgesproken gevoelens van anderen
- Bemerkt (onderhuidse) spanningen, weerstanden of conflictsituaties in een groep en maakt deze bespreekbaar
- Schat in complexe situaties de verschillende belangen en gevoeligheden in

- Houdt rekening met de (politieke) invloeden binnen een organisatie
- Voelt aan wat belangrijk is voor de (politieke) opdrachtgever en speelt daar met respect voor het algemeen belang op in

Oordeelsvorming

Meningen uiten en zicht hebben op de consequenties ervan, op basis van een afweging van relevante criteria

Niveau 3 – Vormt een geïntegreerd 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

Plannen en organiseren

Op effectieve wijze doelen en prioriteiten bepalen en de nodige acties, tijd en middelen aangeven om deze op een efficiënte wijze te kunnen bereiken

Niveau 3 – Plant en organiseert het werk dat zijn afdeling of entiteit overstijgt

- Vertaalt een langetermijnplanning in fasen en/of (deel)projecten en benoemt daarbij de subdoelen
- Coördineert en overziet het werk van diverse onderdelen en schat in wat dit voor het totaal betekent
- Ziet toe op een efficiënte en effectieve besteding van middelen
- Past plannen aan wijzigende omstandigheden aan en houdt daarbij de oorspronkelijke doelen voor ogen
- Anticipeert op ontwikkelingen die van invloed zijn op de doelen van de organisatie en houdt daar in de planning rekening mee

Delegeren

Taken en verantwoordelijkheden doorgeven, rekening houdend met de competenties, interesses, ambitie en ontwikkeling van medewerkers. De gedelegeerde taken opvolgen

Niveau 3 – Delegeert ruime verantwoordelijkheidsgebieden

- Creëert betrokkenheid en verhoogt de eigenwaarde van medewerkers door hen de volle verantwoordelijkheid te geven over bepaalde dossiers, processen, structuren … en over de middelen om de vastgestelde output te bereiken
- Geeft medewerkers bevoegdheid om in complexe en onvoorspelbare situaties autonoom te handelen
- Geeft medewerkers het vertrouwen en het mandaat om zaken op hun manier te realiseren
- Weet waar de sterke kanten van medewerkers liggen en vertrouwt erop
- Zorgt voor autonomie zodat medewerkers hun capaciteiten en ambities kunnen ontplooien

Richting geven

Aansturen en motiveren van medewerkers zodat ze hun doelstellingen en die van de entiteit kunnen realiseren, zowel individueel als in teamverband

Niveau 3 – Geeft richting, zowel via processen en structuren als via het bepalen en uitdragen van een visie

- Communiceert op regelmatige momenten over de opdracht van de entiteit of de organisatie en over het belang daarvan (de missie van de entiteit of organisatie)
- Geeft richting of sturing aan een team of entiteit door een duidelijk en inspirerend beleid uit te dragen (geeft aan waar de organisatie naartoe wil)

- Bepaalt haalbare en uitdagende doelstellingen en doet beroep op het talent van de medewerkers om ze te realiseren
- Introduceert nieuwe structuren, processen en procedures om het beleid te realiseren
- Inspireert als leider vanuit de waarden en doelstellingen van de Vlaamse overheid

Klantgerichtheid

Wensen en behoeften van de verschillende belanghebbenden binnen en buiten de organisatie onderkennen en er adequaat op reageren

Niveau 3 – Optimaliseert de dienstverlening van de organisatie aan belanghebbenden via structurele acties

1. Legt voor zijn entiteit meetbare doelstellingen vast op het vlak van klantgerichtheid en klanttevredenheid
2. Zet systemen op om een kwaliteitsvolle aanpak te garanderen
3. Past diensten, procedures en structuren aan om beter aan toekomstige behoeften en verwachtingen van belanghebbenden te beantwoorden
4. Onderneemt extra acties om de relatie met belanghebbenden op te bouwen en/of te bestendigen
5. Stimuleert en faciliteert anderen om de klantgerichtheid van hun aanpak voortdurend in vraag te stellen en te verbeteren