FUNCTIEBESCHRIJVING
Veiligheidsconsulent

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

<u>Juridische context</u>
Het besluit van de Vlaamse Regering van 15 mei 2009 betreffende de veiligheidsconsulenten geeft uitvoering aan artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer (e-govdecreet), nl. het bepalen van de opdrachten en de manier van aanwijzing van die veiligheidsconsulenten. De Memorie van Toelichting bij het voornoemde artikel 9 van het e-govdecreet verduidelijkt dat bij de verdere omschrijving van de taken van de veiligheidsconsulenten de strengste voorwaarden die bij de Kruispuntbank van de Sociale Zekerheid (KSZ) gelden, eveneens voor de Vlaamse veiligheidsconsulenten zullen gelden. Vandaar dat in het specifieke uitvoeringsbesluit de bepaling van de opdrachten en de aanwijzingsvereisten zijn omschreven naar analogie met de KSZ-wet van 15 januari 1990 en het KB van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid.

De verplichting tot het aanstellen van een veiligheidsconsulent wordt in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer (e-govdecreet), vastgelegd voor elke instantie die:

- persoonsgegevens verwerkt,
- authentieke gegevensbron beheert,
- tussenkomt bij mededeling van persoonsgegevens,
- ondersteunt bij gebruikers- en toegangsbeheer.

De veiligheidsconsulent moet aangesteld worden door de directie, dagelijkse leiding van de organisatie. De veiligheidsconsulent moet ook rapporteren aan de directie. Een veiligheidsconsulent (of zijn adjuncten) wordt pas aangesteld na gunstig advies van de Vlaamse Toezichtcommissie.

<u>Doel</u>

De veiligheidsconsulent adviseert de verantwoordelijke voor het dagelijks bestuur van zijn instelling, op diens verzoek of op eigen initiatief, omtrent alle aspecten van de informatieveiligheid. Hij heeft een adviserende, stimulerende, documenterende en controlerende opdracht inzake informatieveiligheid.

3. AANSTURING

Rapporteert hiërarchisch aan	Leidend ambtenaar	
Rapporteert functioneel aan	ICT-manager / ICT-directeur	
Stuurt hiërarchisch aan	/	**Niet van toepassing** < 5 medewerkers 5-15 medewerkers +15 medewerkers
Stuurt functioneel aan	Alle (ICT-gerelateerde) functies die in het kader van opzet van nieuwe en verbetering van bestaande toepassingen rekening moeten houden met informatieveiligheidsaspecten	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 leidend ambtenaar
- Planningshorizon van minstens 3 jaar (oa ifv het verplichte veiligheidsplan).
- Heterogene groep van belanghebbenden, gezien informatieveiligheid verschillende (ICT) processen en projecten doorkruist

5. AUTONOME BESLISSINGSBEVOEGDHEID

- Moet onafhankelijk en onpartijdig kunnen opereren
- Autonoom bevoegd voor het uittekenen van een veiligheidsbeleid, inclusief alle richtlijnen en standaarden.

6. RESULTAATGEBIEDEN

RESULTAATGEBIED 1 : Veiligheidsbeleid uittekenen

Doel : Ontwerpen en implementeren van een veiligheidsbeleid met als doel over een duidelijke methodiek en aanpak te beschikken inzake informatie- en ICT-veiligheid binnen de organisatie, dit zowel qua fysieke als elektronische informatieveiligheid.

Deelactiviteiten :

- ✓ Procedures opstellen en onderhouden inzake informatieveiligheid (zowel algemeen als voor een specifieke doelgroep en/of voor bepaalde informatiesystemen)
- ✓ Documenteren en onderhouden van de verschillende procedures inzake informatieveiligheid
- ✓ Continu zoeken naar nieuwe oplossingen inzake informatieveiligheid om het beleid van de informatiebeveiliging te optimaliseren.
- ✓ Opstellen van een veiligheidsplan – dit rechtstreeks in opdracht van de leidend ambtenaar van de organisatie – voor een termijn van drie jaar, met vermelding van de middelen op jaarbasis die vereist zijn om het plan uit te voeren.

- ✓ Jaarlijkse evaluatie, rapportering en bijsturing van het organisatiebrede veiligheidsplan.
- ✓ …

RESULTAATGEBIED 2 : Risicobeoordeling en risicobehandeling

Doel : Continu beoordelen van de beveiligingsrisico's en -behoeften rond de informatie die eigen zijn aan de organisatie en die het gebruik en de verwerking van persoonsgegevens betreffen, teneinde de nodige beheersmaatregelen te kunnen nemen.

Deelactiviteiten :

- ✓ Analyseren van de huidige en toekomstige risico's inzake informatie en informatiesystemen om structurele risico's te vermijden of tot een aanvaardbaar niveau te reduceren.
- ✓ Inbreuken onderzoeken op de beveiligingsprocedures om de lekken in de beveiliging te vinden en problemen in de toekomst te vermijden.
- ✓ Tests (laten) uitvoeren om de risico's inzake veiligheid naar de toekomst te kunnen inschatten en bijsturen waar nodig.
- ✓ …

RESULTAATGEBIED 3 : Toezicht en controle

Doel : Toezien op en controleren van de logische en fysieke beveiliging van gegevens, teneinde de dagdagelijkse veiligheid inzake de uitwisseling van privacygevoelige gegevens (informatieveiligheid) te kunnen verzekeren.

Deelactiviteiten :

- ✓ Controleren en opvolgen of de procedures inzake informatieveiligheid worden gevolgd om een coherent beleid inzake informatieveiligheid binnen de organisatie na te leven.
- ✓ Toezien dat de verschillende verantwoordelijkheden inzake veiligheid (preventie, toezicht, opsporing en verwerking) duidelijk in kaart zijn gebracht
- ✓ Toezien op het feit dat de personen belast met de veiligheid in alle onafhankelijkheid kunnen handelen en ervan gevrijwaard blijven dat ze voor persoonlijke - of tegenstrijdige belangen onder druk worden gezet.
- ✓ …

RESULTAATGEBIED 4 : Communicatie en overleg

Doel : Plegen van communicatie en overleg met alle mogelijke betrokken partijen met als doel een draagvlak en gedeeld begrip en toepassing inzake informatieveiligheid

Deelactiviteiten :

- ✓ plegen van continu overleg met het management
- ✓ communiceren over de bestaande behoeften, mogelijke blinde vlekken en verbeteringsmogelijkheden
- ✓ bijwonen van verschillende overlegfora (management, project, experten, etc.)
- ✓ advies verlenen inzake informatieveiligheid aan de leidend ambtenaar
- ✓ in het kader van projecten om de klanten in staat te stellen
- ✓ In het kader van ICT-projecten toezien op de aspecten inzake informatieveiligheid om de risico's inzake informatieveiligheid tot een minimum te beperken.
- ✓ Organisatiebreed verlenen van advies inzake informatieveiligheid en sensibilisatie.
- ✓ …

RESULTAATGEBIED 5 : Kennis mbt het vakgebied

Doel : Bijhouden van trends en ontwikkelingen in het vakgebied en de regelgeving om een juridisch correct en performant veiligheidsbeleid na te streven.

Deelactiviteiten :

- ✓ Studiewerk verrichten om de recentste evoluties en verplichtingen op het werkveld en de werkmethoden te kennen.
- ✓ Onderzoeken van toepasbaarheid van nieuwe methoden en technologieën.
- ✓ Meewerken aan de uitbouw van kennisbeheer rond informatieveiligheid.
- ✓ De organisatie vertegenwoordigen op diverse fora rond informatieveiligheid.
- ✓ Een actieve bijdrage leveren aan de veranderingen noodzakelijk voor de verdere professionalisering en verhoging van de kwaliteit van informatieveiligheid in de organisatie
- ✓ …

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

7. CONTACTEN

- **INTERNE CONTACTEN**

Uitwisselen van informatie : projectmedewerkers, medewerkers en belanghebbenden binnen de ganse organisatie

Onderhandelen met : Business verantwoordelijken en managementleden, ICT-architect, programma-manager, projectleider

- **EXTERNE CONTACTEN**

Uitwisselen van informatie : Breed professioneel netwerk

Onderhandelen met : Leveranciers van producten of diensten

8. FUNCTIONERINGSCRITERIA

1. Gewenst minimaal opleidingsniveau (niet vereist) : Hoger onderwijs van het lange type (master), bij voorkeur in een ICT-gerelateerde richting.

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	x	x	
4j – 7j			
>7 jaar			

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	x
IT Strategy and Planning	
Business Process Analysis	
Business Process Improvement	
Security and Risk Management	x
Program and Project Management	x
Architecture Management	x
Business Relationship Management	x
Infrastructure and Operations	x
Customer Service (Help Desk)	
Application Development and Management	x
Sourcing management	x
Vendor management	x
ICT Human Resources	
ICT Finance	

4. Gedragscompetenties

Analyseren

Een probleem duiden in zijn verbanden en op een efficiënte wijze op zoek gaan naar aanvullende relevante informatie

Niveau 2 – Legt verbanden en ziet oorzaken

- Benadert het probleem of vraagstuk vanuit verschillende gezichtspunten
- Legt verbanden tussen verschillende soorten informatie
- Benoemt de oorzaken van problemen
- Detecteert onderliggende problemen
- Integreert nieuw gevonden informatie met bestaande informatie

Zorgvuldigheid

Handelen met aandacht voor kwaliteit en gericht op het voorkomen van fouten

Niveau 3 – Neemt verantwoordelijkheid over de kwaliteit van het werk van anderen

- Benoemt kwaliteitscriteria voor de organisatie en zorgt dat anderen deze kennen
- Bewaakt de kwaliteit van het werk van anderen en maakt hen attent op fouten
- Analyseert de oorzaak van gesignaleerde afwijkingen en stelt oplossingen voor om deze te voorkomen
- Ontwikkelt en bewaakt systemen en procedures gericht op het voorkomen van onnauwkeurigheden
- Is alert op mogelijkheden tot verbetering op detailniveau

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 2 – Coördineert het eigen werk en dat van anderen

- Structureert informatie, situaties en problemen en handelt deze efficiënt en effectief af

- Weet wat er aan tijd, mensen en middelen nodig is om het gewenste resultaat te behalen
- Maakt een helder plan voor de eigen en andermans werkzaamheden met doelen en activiteiten (concreet, volledig, overzichtelijk)
- Verdeelt werkzaamheden en maakt afspraken met de betrokkenen over de uitvoering
- Bouwt meetmomenten in om de voortgang van het werk te volgen

Coachen

Anderen ondersteunen en begeleiden zodat ze zich professioneel en persoonlijk kunnen ontwikkelen en de effectiviteit en efficiëntie van hun werk verhoogt

Niveau 1 – Ondersteunt bij het behalen van resultaten

- Maakt de verwachtingen duidelijk en legt uit hoe opdrachten kunnen uitgevoerd worden en waarom
- Moedigt anderen aan om nieuwe taken te leren en om zich te vervolmaken in hun job
- Geeft duidelijke en constructieve feedback over het functioneren
- Geeft aanwijzingen en tips om resultaten te verbeteren
- Heeft zicht op wat iemand kan en houdt bij het leerproces rekening met zijn talenten en beperkingen

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, …)

Gelezen en goedgekeurd,
Naam + handtekening
Functiehouder

Gelezen en goedgekeurd,
Naam + handtekening
Verantwoordelijke

Gelezen en goedgekeurd,
Naam + handtekening
Directie