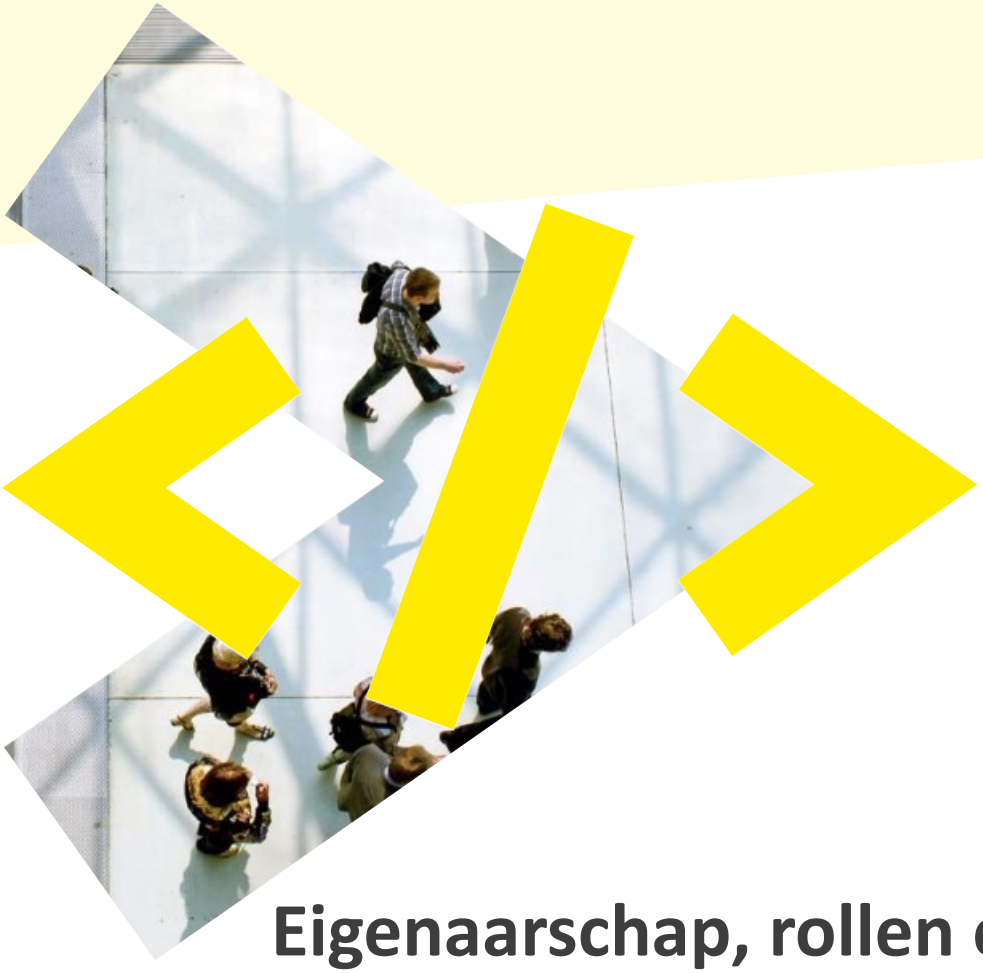
Behorende bij het Informatieclassificatieraamwerk van de Vlaamse overheid

Vlaamse overheid



Eigenaarschap, rollen en verantwoordelijkheden voor Informatieveiligheid

Versie: maart 2023

Bron: Team Informatieveiligheid

Doelgroep: Entiteiten die rollen voor informatieveiligheid inrichten

DIGITAAL VLAANDEREN

Voor een **veilige** digitale overheid

Informatieveiligheid is de verantwoordelijkheid van alle medewerkers

DIGITAAL VLAANDEREN

Binnen de Vlaamse overheid is het de taak van iedere entiteit die gegevens verwerkt om rollen, verantwoordelijkheden en bevoegdheden die belangrijk zijn voor Informatieveiligheid, te definiëren, communiceren en toe te wijzen. Binnen het organiseren van Informatieveiligheid zijn er naast voltijdse functies, ook rollen en verantwoordelijkheden die onderdeel uitmaken van een breder takenpakket.

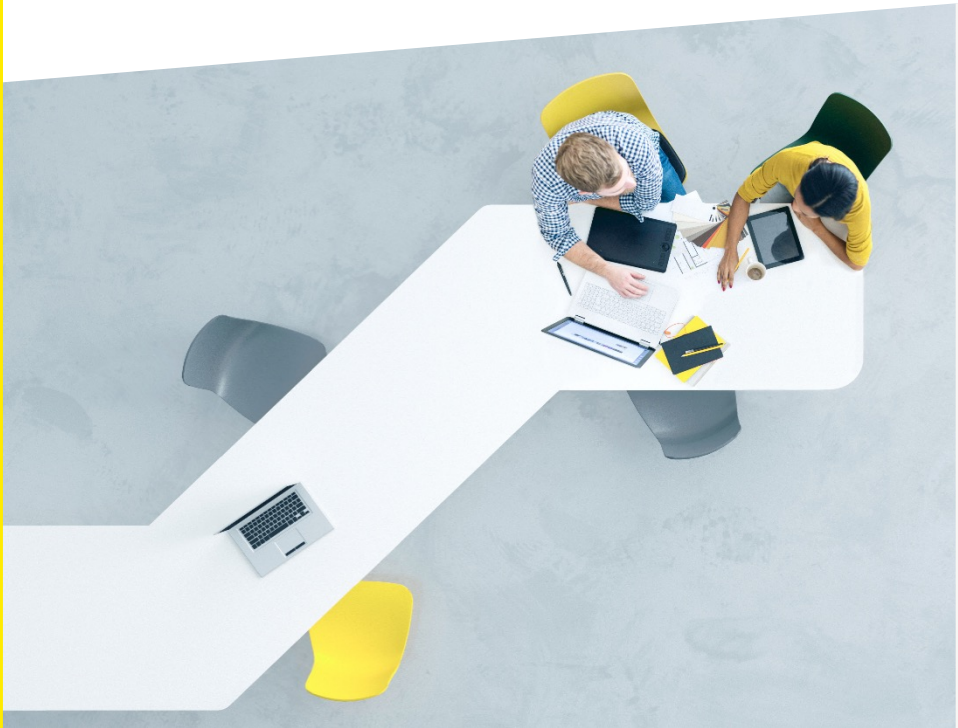
Deze handreiking geeft een overzicht van de meest voorkomende rollen en verantwoordelijkheden die georganiseerd moeten worden. Een aantal ervan zijn onmisbaar, zoals de aansprakelijke eigenaar en de gedelegeerde verantwoordelijken voor beleidsvorming en toezicht op een adequate inrichting van Informatieveiligheid.

Omdat iedere organisatie anders is, moeten deze voorbeeldrollen aangepast worden en waar nodig vastgelegd in goed omschreven functies. De implementatie moet georganiseerd worden in overeenstemming met het beleid van de entiteit.

Hierbij dienen minimaal de volgende verantwoordelijkheden te worden toegewezen:

- *Vorming en beheer van het Informatieveiligheidsbeleid en het toezicht op naleving*
- *Communicatie van het beleid en bewustwording van specifieke veiligheidsonderwerpen*
- *Uitvoering van Informatieklassebepalingen en risicoanalyses en het beheer van risico's*
- *Selectie, ontwikkeling, implementatie en het beheer van beheersmaatregelen*
- *Controle op de effectiviteit van beheersmaatregelen*

Deze handreiking heeft als doelgroep directies en security officers (of informatieveiligheidsconsulenten) en is een handleiding voor de inrichting van eigenaarschap, rollen en verantwoordelijkheden voor Informatieveiligheid.



Raadpleeg het Informatieclassificatie raamwerk voor meer informatie en voorbeelden van rollen **via deze QR:**

Overzicht van belangrijke rollen voor Informatieveiligheid

DIGITAAL VLAANDEREN

 **Leidend ambtenaar, Administrateur-generaal**	De hoogste ambtenaar van een entiteit is eigenaar en aansprakelijk voor beleidsvorming en uitvoering van het informatieveiligheidsbeleid en de compliance met het Informatieclassificatieraamwerk (ICR) van de Vlaamse overheid (dit is verplicht voor entiteiten binnen de Vlaamse administratie).
 **Eigenaar van proces, product of dienst**	Gedelegeerde eigenaren zoals afdelings-, diensthoofden of andere lijnmanagers zijn verantwoordelijk voor de vertaling en uitvoering van het informatieveiligheidsbeleid naar veilige processen, producten en diensten inclusief informatieklasse bepalingen, risicoanalyses en beheersmaatregelen.
 **Programma-, Projectmanager, Scrum master**	Een Programma- en Projectmanager of Scrummaster dragen zorg voor de vertaling van het beleid naar *Secure en Privacy by Design* oplossingen en compliance met de van toepassing zijnde wet- en regelgeving. Dit in de ontwikkeling, oplevering en overdracht naar operationeel beheer van veilige processen, producten en diensten.
 **Architect, Ontwerper**	Een Architect of Ontwerper is verantwoordelijk voor de definitie, selectie en ontwerp van beheersmaatregelen in architectuur en functionele en technische ontwerpen in lijn met de vastgestelde informatieklasse, risicoprofiel en standaarden voor security architectuur en data management.
 **Ontwikkelaar, Programmeur**	Een Ontwikkelaar of Programmeur is verantwoordelijk voor de ontwikkeling en implementatie van beheersmaatregelen in lijn met de voorgeschreven architectuur en functionele en technische ontwerpen inclusief het volgen van (industrie)richtlijnen voor de ontwikkeling van veilige infrastructuur, systemen en applicaties.
 **Operationeel beheerder, Service delivery manager**	Een Operationeel beheerder of Service delivery manager is verantwoordelijk voor de operatie, het beheer en monitoring van de effectiviteit van beheersmaatregelen binnen processen, producten en diensten in lijn met het vastgestelde beleid en (veiligheid)procedures.
 **Chief Information Security Officer of Consulent**	De Chief Information Security Officer of Consulent heeft de leidende rol in beleidsvorming, toezicht op naleving en onafhankelijke controletoetsing (namens de directie), advisering en ondersteuning, bewustzijnscampagnes, overkoepelende risicoanalyses en –aggregatie en rapportering.
 **Data Privacy Officer, Functionaris Gegevens-bescherming**	De Data Privacy Officer of Functionaris Gegevens-bescherming is verantwoordelijk voor de bescherming van persoonsgegevens en privacy. De taken zijn vastgelegd in een regeringsbesluit. Een nauwe samenwerking met de Security officer is wenselijk. Een entiteit kan er voor kiezen om deze twee rollen te combineren in één functie zolang de onafhankelijkheid maar gewaarborgd blijft.

Overzicht van belangrijke rollen voor Informatieveiligheid

DIGITAAL VLAANDEREN

Inkoper	Een Inkoper is verantwoordelijk voor de borging van afspraken in contracten met leveranciers over Informatieveiligheid en compliance rapportage, zoals gedefinieerd door de Eigenaar voor specifieke eisen en door de CISO voor algemeen beleid. Hij staat ook in voor het beheer van standaardsjablonen voor informatieveiligheidsclausules in contracten.
Contract-, Leveranciers-manager	Een Contract-of Leveranciersmanager is verantwoordelijk voor het beheren van contractuele afspraken met leveranciers over Informatieveiligheid en compliance, inclusief het definiëren van performance indicatoren en het actief opvolgen van informatieveiligheidsrapportages in afstemming met de eigenaren van de uitbestede producten en diensten.
Jurist	Een Jurist adviseert inkopers, eigenaren en/of contract- en leveranciersmanagers over de wet- en regelgeving die van toepassing is. Hij monitort actief en adviseert over opkomende veranderingen betreft wet- en regelgeving in de context van Informatieveiligheid.
HR-medewerker, Recruiter	Een HR-medewerker of Recruiter is verantwoordelijk voor het borgen van afspraken over Informatieveiligheid in arbeids- en inhuurcontracten en geheimhoudingsverklaringen, ook voor het beheer en de begeleiding van disciplinaire procedures en screening van gevoelige posities.
Medewerker facilitaire zaken	Een Medewerker facilitaire zaken is verantwoordelijk voor fysieke beveiliging van gebouwen en andere facilitaire zaken, inclusief logische toegangscontrole en het monitoren van de naleving en effectiviteit van fysieke beheersmaatregelen.
Informatie-veiligheids-specialist	Een Informatieveiligheidsspecialist heeft een gespecialiseerde (technische) security rol met verschillende taken naast de leidende rol van de CISO. Hij is verantwoordelijk voor de ondersteuning van projecten en operationele beheerafdelingen bij de ontwikkeling, het beheer of review van veilige producten en diensten.
Auditor, Risico-beheerder	Een Auditor heeft een onafhankelijke rol in het leveren van objectieve assurance en adviezen aan directies over de toereikendheid en effectiviteit van governance en risicobeheer. Optioneel kan er een risicocoördinator aangesteld zijn die overzicht heeft over het risicobeheer en dit kan beoordelen en rapporteren aan de directie vanuit een tweedelijnsrol.
Lijnmanagers en alle medewerkers	Lijnmanagers zijn verantwoordelijk voor het toezicht op informatieveiligheidsbewustzijn en naleving van het beleid door hun afdelingen en teams. Iedere medewerker is zelf ook verantwoordelijk om proactief kennis te nemen van het beleid, deze na te leven en incidenten, risico's en opportuniteiten te melden.

Toelichting

DIGITAAL VLAANDEREN

PRIMAIRE EN SECUNDAIRE ROLLEN

Informatieveiligheid is in eerste instantie de verantwoordelijkheid van het (lijn-)management.

Informatieveiligheidsrollen, zoals een CISO, ondersteunen het management daarbij.

De manager is degene die verantwoord kan beslissen over de mogelijk tegenstrijdige belangen tussen Informatiebeveiliging, efficiëntie in de procesvoering en de gebruiksvriendelijkheid van informatiesystemen.

De manager is ook het beste gepositioneerd om de waarde van de informatie(verwerking) en mogelijke business impact vast te stellen en is daarmee dan ook indirect de risico-eigenaar.

Informatieveiligheid is niet los te denken van de context (proces, product of dienst) waarin maatregelen moeten functioneren. Dat maakt dat er geen afzonderlijke verantwoordelijkheden zijn te definiëren en te beleggen bij personen die buiten de context van proces, product of dienst opereren.

Een uitzondering hierop zijn centrale infrastructuurdiensten waarop applicaties kunnen zijn aangesloten, zoals bijvoorbeeld toegangscontrole waarbij het technische beheer in een ander team zit. De eigenaar van de aangesloten applicatie blijft wel verantwoordelijk voor het beheer en de validatie van de personen die toegang tot deze applicatie hebben.

Een CISO of veiligheidsconsulent biedt advies en ondersteuning bij bijvoorbeeld informatieklassebepalingen, risicoanalyses en beheersmaatregelen. Dit naast de verantwoordelijkheid voor beleidsvorming, dreigingsanalyses, overzicht en aggregatie van risico's en toezicht op naleving.
Een CISO heeft ook vaak het mandaat om te interveniëren indien te hoge informatieveiligheidsrisico's worden genomen.

Op het portaal van het Informatieclassificatieraamwerk vindt u een voorbeelddocument van deze rollen verantwoordelijkheden.

SCHEIDING VAN TAKEN

Wetgeving en normen verwachten vaak scheiding in de verantwoordelijkheid voor beleid en advies tegenover implementatie en uitvoering.

Een rol die primair adviseert en anderen ondersteunt bij de implementatie van maatregelen kan niet onafhankelijk en objectief vaststellen of de juiste maatregelen zijn getroffen, omdat hij dan zijn eigen adviezen kan tegenkomen.

In de definitie van rollen moet er gezorgd worden voor tegengestelde belangen en taken en dit in het belang van Informatieveiligheid.

Dit geldt niet alleen voor veiligheidsrollen, maar ook in het kader van ontwerp, ontwikkeling, implementatie en operatie van processen en systemen.

TOEZICHT versus CONTROLE

Toezicht houden is iets anders dan controleren.
Toezicht op de naleving van beleid vindt plaats door waarneming, gesprekken met betrokkenen of door documentatie te bestuderen.

Toezicht is er niet primair op gericht een objectief en onafhankelijk oordeel te geven.

Er is (vanwege compliance met wetgeving en normen) behoefte aan objectieve oordeelsvorming over de effectieve werking van maatregelen door een onafhankelijke interne of externe rol met de juiste audit en/of technische vakkennis.

Dit is belangrijk om een papieren werkelijkheid te vermijden en een vals gevoel van veiligheid te voorkomen.

In de definitie van rollen moet rekening gehouden worden met dit verschil.