Vlaamse Regering

De Vlaamse minister van Buitenlandse Zaken, Cultuur, Digitalisering en Facilitair Management

NOTA AAN DE VLAAMSE REGERING

Betreft: Strategie voor Informatieveiligheid

De Vlaamse Regering wenst de strategie rond informatieveiligheid te versterken om een antwoord te bieden op de uitdagingen en opportuniteiten met betrekking tot een veilige informatieverwerking binnen de Vlaamse overheid.

Met deze nota vragen we bevestiging aan de Vlaamse Regering van de strategie rond Informatieveiligheid zoals voorgesteld door het Stuurorgaan voor Informatie- en ICT-Beleid

1. SITUERING

A. INFORMATIEVEILIGHEID BINNEN DE VLAAMSE OVERHEID

Informatieveiligheid (inclusief de bescherming van persoonsgegevens) is geen opdracht die op zichzelf staat. Informatieveiligheid maakt deel uit van het DNA van de Vlaamse overheid. Het vormt een ondeelbaar geheel met de manier waarop we iedere dag omgaan met informatie, tijdens elke activiteit op de werkvloer, tijdens elk contact met de burger, bedrijven, overheden en entiteiten. Hoe triviaal deze interacties soms lijken te zijn, telkens is er wisselwerking aan informatiestromen en processen die de noodzakelijke beschermende maatregelen verantwoorden, op maat van de toepassing en het achterliggende proces.

Deze nota wil een antwoord bieden op de toenemende dreiging van cybercriminelen en ervoor zorgen dat de Vlaamse overheid een betrouwbare partner is én blijft op het vlak van informatieveiligheid.

De toenemende digitalisering introduceert immers in toenemende mate een aantal risico's voor onze werking:

- Onze informatie-verwerkende applicaties en infrastructuur zijn onmisbaar om onze bestuurstaken uit te voeren. Onderbrekingen van de bereikbaarheid, integriteit en vertrouwelijkheid van deze systemen kunnen een grote impact hebben op onze werking en onze dienstverlening aan de gemeenschap.

- Steeds meer toestellen en gespecialiseerde toepassingen worden verbonden binnen onze informatieverwerking. Toestellen in eigen beheer, maar ook in toenemende aantallen die verbonden worden via het internet. Dit biedt nieuwe opportuniteiten, maar deze 'verbondenheid' verhoogt eveneens onze kwetsbaarheid bij aanvallen en misbruiken door het

hogere risico potentieel dat voortkomt uit een meer waarschijnlijke en snellere verspreiding van veiligheidsincidenten.

- Hoge complexiteit van de ICT-systemen: vele publieke entiteiten zijn afhankelijk van complexe en vaak verouderde ICT-systemen. Deze hard- en softwarecomponenten zijn niet ontworpen om nieuwe dreigingen af te wenden. Ook de processen die de beschikbaarheid en integriteit van deze systemen te garanderen presteren vaak onder het vereiste beveiligingsniveau.

- Cyberaanvallen kunnen eenvoudig en goedkoop worden uitgevoerd: de brede commerciële beschikbaarheid van hacking-tools op het internet betekent dat iedereen die een systeem wil hacken dit relatief eenvoudig, goedkoop en zonder gespecialiseerde kennis kan uitvoeren.

- Beperkt veiligheidsbewustzijn is een onderkend probleem: het gebrek aan kennis en vaardigheden vormen een significante kwetsbaarheid op zich, die kan worden uitgebuit door derde partijen. Het gedrag m.b.t. veiligheid van leidinggevenden en werknemers is cruciaal om een gepast niveau van bescherming te bereiken.

De nota beschrijft de strategie met voorgestelde doelstellingen, leidende principes en aanpak met betrekking tot informatieveiligheid binnen de Vlaamse overheid en binnen de dienstverlening aangeboden aan de Vlaamse overheid.

De voorgestelde proactieve aanpak stuurt de Vlaamse overheid bij de identificatie van individuele en gemeenschappelijke behoeften en uitdagingen. De uitvoering van deze visie steunt op samenwerking tussen de Vo entiteiten onderling, gesteund door externe partners in combinatie met doordachte en efficiënte investeringen. Dit voorziet de Vlaamse overheid van adequate mechanismes om op dreigingen binnen zijn informatieverwerking te reageren.

Deze benadering bouwt verder op bestaande overlegstructuren, bestaande compliance vereisten en afgelijnde verantwoordelijkheden, zowel op vlak van risicobeheer als operationeel. Op die manier bekomen we een kostefficiënte duurzame aanpak en bereiken we een gepast beveiligingsniveau. Een sleutelelement binnen de visie bestaat uit het identificeren en invullen van ontbrekende capaciteiten en kennisprofielen. Deze efficiëntie zal bereikt worden via een gemeenschappelijke en gedeelde dienstverlening.

B. TOEPASSINGSGEBIED

De scope van deze strategie en het daaruit voortvloeiende informatieveiligheidsbeleid is de Vlaamse administratie zoals bepaald in het bestuursdecreet van 7 december 2018. Waar er uitwisseling van informatie nodig is met andere overheidsinstanties, waaronder de lokale besturen, wordt beroep gedaan op protocollen, zoals voorzien in het e-govdecreet van 18 juli 2008 (decreet betreffende het elektronische bestuurlijke gegevensverkeer).

C. BELEIDSKADER

Het Regeerakkoord van de Vlaamse Regering 2019-2024 stelt dat de digitalisering een nieuwe fase intreedt, waarbij alles met alles en iedereen met iedereen verbonden is. Digitaliseringsinitiatieven in verschillende beleidsdomeinen moeten dan ook meer dan ooit op elkaar afgestemd worden. Interbestuurlijke samenwerking is hierbij het antwoord. De Vlaamse Regering wil dan ook van innovatie en digitale transformatie een speerpunt van haar beleid maken.

De Vlaamse Regering heeft zich in het bijzonder tot doel gesteld dat de Vlaamse administratie en lokale overheden ook radicaal digitaal gaan, om een “state of the art”-dienstverlening aan de burgers,

ondernemingen en verenigingen te kunnen leveren, met zo weinig mogelijk paperassen en met nodige aandacht voor de mensen die nog niet mee zijn met de digitale trein. Om dit te realiseren stelt het Regeerakkoord dat de investeringen in de digitalisering van de overheidsprocessen zullen verhoogd worden, waarbij ingezet wordt op de gebruiksvriendelijkheid van de bestaande digitale platformen en de agenda Radicaal Digitaal ambitieus wordt verdergezet.

Informatieveiligheid is bovendien een speerpunt in het strategisch plan van het Stuurorgaan Vlaams Informatie- en ICT-beleid, zoals vastgelegd in het Bestuursdecreet van 7 december 2018. De Vlaamse Regering keurde op 26 juni 2020 de prioriteiten goed van het strategisch plan samen met de prioriteiten van het Vlaanderen Radicaal Digitaal 2-programma. Het stuurorgaan kan, binnen de krijtlijnen van het strategisch plan, technische voorschriften en richtlijnen voor de Vlaamse administratie en de lokale overheden vastleggen over de aanmaak, het beheer, de uitwisseling, het gebruik, het hergebruik en de archivering van de gegevens en diensten van de Vlaamse administratie en de lokale overheden met het oog op de realisatie van een efficiënt en interoperabel gebruik van gegevens.

Deze strategie biedt eveneens aan de adviezen die werden geformuleerd aan het Stuurorgaan door Audit Vlaanderen d.m.v. thema-audit informatiebeveiliging/ Opdrachtnummer 1401 02 met betrekking tot het opstellen van een Vo-brede strategie rond informatieveiligheid.

D. GEVOLGDE WERKWIJZE

Een sneuveltekst is opgesteld door het ICT- en Informatieveiligheidsteam van Het Facilitair Bedrijf en voorgesteld als begin voor een open en transparant debat in het Stuurorgaan Informatie- en ICT-Beleid. Daar zijn deelnemers bepaald die een brede basis vormen binnen de Vlaamse overheid om deel te nemen aan een Taakgroep.

Deze Taakgroep heeft in 5 verschillende sessies het volledige Strategiedocument doorgenomen, besproken en waar nodig aangepast aan de wensen en gevoeligheden van de verschillende werkgebieden en entiteiten.

Het resultaat is opnieuw voorgelegd aan het Stuurorgaan Informatie- en ICT-Beleid ter validatie en goedgekeurd.

2. DOELSTELLINGEN

De Vlaamse overheid wil met deze strategie volgende doelstellingen[1] bereiken:

- Het vertrouwen genieten van de burger, onderneming en/of vereniging.
- De persoonlijke levenssfeer van de burger beschermen.
- De reputatie hoog houden van de Vlaamse overheid als betrouwbare partner.
- Bedrijfscontinuïteit garanderen tijdens en na een ernstig incident
- Een innovatieve kracht zijn.

3. STRATEGISCHE PRINCIPES

Deze strategie is gebaseerd op volgende strategische uitgangspunten:

1 Bron: Centrum voor cybersecurity – Baseline security guidelines

〉 **Subsidiariteit en verantwoordelijkheden**

We houden rekening met de aansprakelijkheden en verantwoordelijkheden van de individuele entiteiten bij het uitvoeren van hun kernactiviteiten. Het beleid respecteert de subsidiariteit en houdt rekening met de diversiteit in de structuur en risicoprofiel van de Vlaamse overheid.

〉 **Proportioneel**

De maatregelen en investeringen op het vlak van informatieveiligheid zijn proportioneel aan het belang van de verwerkte informatie, gebaseerd op een gewogen risicoanalyse. Welke maatregelen en controles exact op welke informatie van toepassing zijn, hangt af van de gevoeligheid van de gegevens.

〉 **Ondersteunend**

Een sterk informatieveiligheidsbeleid zorgt voor een veilig gebruik van moderne, nieuwe en innovatieve technologie, die de Vlaamse overheid in staat stelt om met vertrouwen haar kerntaken uit te voeren in de hedendaagse samenleving.

〉 **Gebaseerd op samenwerking, gezamenlijke doelstellingen en objectieven**

Incidenten bij individuele entiteiten hebben potentieel grote impact op de volledige Vlaamse overheid. Gezien elke entiteit worstelt met identiek dezelfde uitdagingen rond informatiebeveiliging nemen we deze uitdaging gezamenlijk op. Hiermee zorgen we voor efficiëntie, brede inzetbaarheid en resultaat.

〉 **Bewezen**

De strategie rond informatieveiligheid is gebaseerd op industrie standaarden en beste praktijken. We maken veiligheid meetbaar, op een manier die controle en bijsturing mogelijk maakt. We brengen vereisten, risico en efficiëntie structureel in kaart en volgen deze op.

〉 **Realistisch en schaalbaar**

Het beleid moet uitvoerbaar zijn voor alle betrokken partijen, rekening houdend met de grootte en slagkracht van individuele entiteiten. We maken maximaal gebruik van bestaande processen.

〉 **Duurzaam**

Informatieveiligheid is een uitdaging die een lange termijn en structurele aanpak vereist met aandacht voor continue verbetering. Het beleid dient verankerd te zijn in de bestuurlijke regelgeving.

4. STRUCTUUR

Het informatieveiligheidsbeleid van de Vlaamse overheid wordt gestuurd door een hiërarchische set van documenten die de principes met betrekking tot informatieveiligheid en de bescherming van persoonsgegevens in de praktijk omzetten. Deze documenten zijn het resultaat van samenwerking tussen de verschillende entiteiten binnen de Werkgroep Informatieveiligheid van het Stuurorgaan.

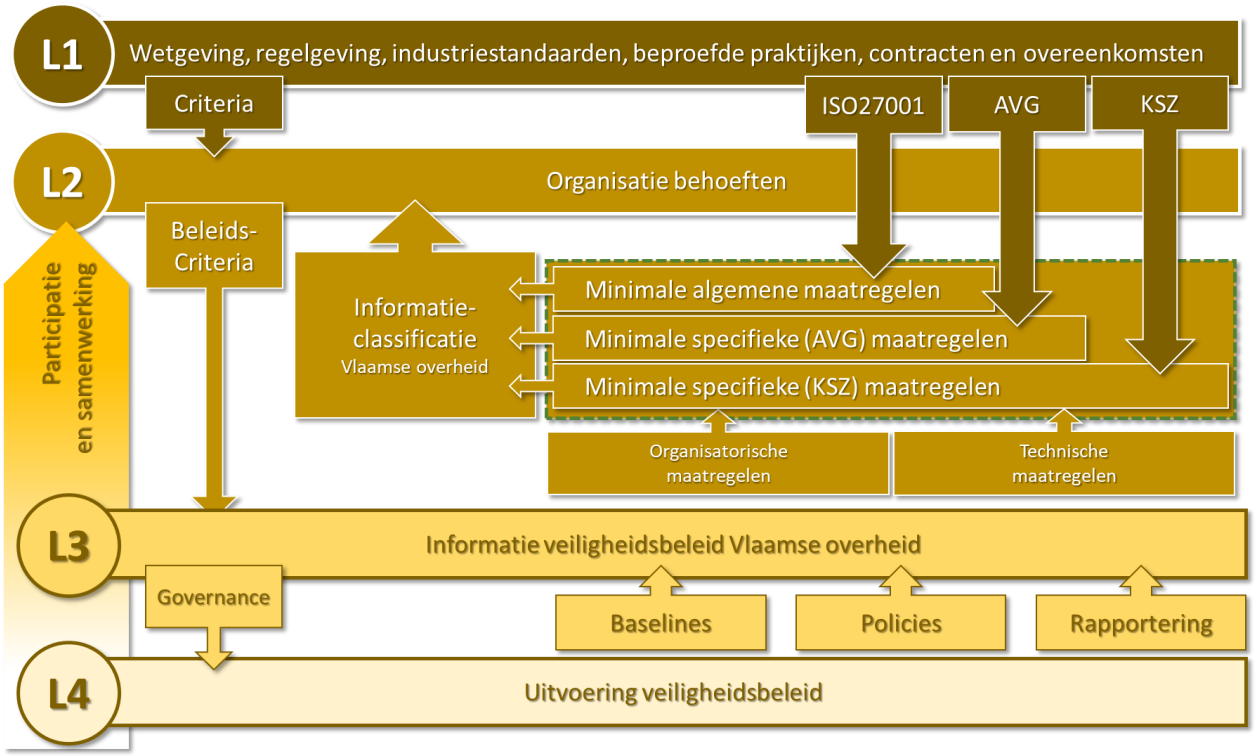
- Deze nota bevat de doelstellingen, leidende principes en rollen/verantwoordelijkheden met betrekking tot informatieveiligheid binnen de Vlaamse overheid.

- Het **strategisch plan** bevat de concrete prioriteiten en doelstellingen met betrekking tot informatieveiligheid. Het definieert het uitvoeringsprogramma met betrekking tot informatieveiligheid met gepaste middelen, opleiding en training, binnen de krijtlijnen van het strategisch plan van het stuurorgaan zoals goedgekeurd door de Vlaamse Regering op 26 juni 2020. Een sleutelelement van het plan van aanpak bestaat uit het identificeren van ontbrekende capaciteiten die efficiënter kunnen worden opgelost via een Vo-brede aanpak.

- Het **Raamwerk voor Vo informatieclassificatie** is de leidraad voor informatiebeveiliging. Op basis van de classificatie van de informatie, bepaalt het de minimummaatregelen die op een gemeenschappelijke manier van toepassing zijn op alle Vlaamse entiteiten in scope van deze nota. Deze maatregelen en beleidscriteria zijn gebaseerd op internationale normen, goede praktijken op het gebied van informatiebeveiliging en de ervaringen van de deelnemers aan de Werkgroep informatieveiligheid.

- De **Minimale maatregelen** vormen de begeleidende documentatie in context van het Vo informatieclassificatie raamwerk. Ze bevatten de concrete kwaliteitseisen waaraan de minimale informatieverwerking moeten voldoen: bv. op het vlak van gebruikers -en toegangsbeheer, fysieke beveiliging, netwerkbeveiliging, incident -en probleembeheer, toegangen voor beheerders , encryptie -en sleutelbeheer … Ze zijn tweeledig:
    - Procesmatige vereisten op vlak van informatieveiligheidsbeheer. Organisatie, beheersing.
    - Kwaliteitseisen aan de veiligheidsmaatregelen, volledigheid van de collectie veiligheidsmaatregelen (geen technische details)

Deze kwaliteitseisen worden verbonden aan de informatieklassen zoals deze zijn beschreven in het raamwerk voor Vo informatieclassificatie.



De Vlaamse Regering geeft, overeenkomstig art. 3 laatste lid van het decreet van 23 december 2016 houdende de oprichting van het stuurorgaan Vlaams Informatie- en ICT-beleid, het mandaat aan het Stuurorgaan, om samen met de werkgroep Informatieveiligheid en het agentschap Digitaal Vlaanderen deze beleidsdocumenten vorm te geven en op te volgen conform de afspraken binnen het organisatiemodel. Deze documenten en de toepassing van de VO-informatieclassificatie zijn bindend voor alle entiteiten van de Vlaamse overheid in scope van de strategie.

5. ROLLEN EN VERANTWOORDELIJKHEDEN

Om de rollen en verantwoordelijkheden scherp te stellen, voeren we het concept ‘eigenaarschap’ in.

We identificeren eigenaar (‘owner’), gedelegeerd eigenaar (‘delegate owner’) en uitvoerder (‘custodian’). In het organisatie model is een eigenaar aansprakelijk (‘accountable’) en zijn de gedelegeerd eigenaar en de uitvoerder verantwoordelijk (‘responsible’). Merk op dat rollen steeds toegewezen worden aan een unieke persoon op basis van zijn/haar organisatorische functie. De entiteiten zijn verantwoordelijk voor de autonome toewijzing van functies, rollen en verantwoordelijkheden binnen de eigen entiteit

Een eigenaar is aansprakelijk voor alle aspecten die te maken hebben met de kernactiviteiten van de entiteit en de hieraan verbonden processen en ondersteunende infrastructuur. Het concept eigenaar is dus niet beperkt tot een toepassing alleen. In de context van informatieveiligheid is de eigenaar aansprakelijk voor de uitvoering van het informatieveiligheidsbeleid. Hij/zij is tevens aansprakelijk voor het beheer van de risico’s van de eigen kernactiviteiten en om het beleid, de afspraken en richtlijnen binnen de eigen entiteit te implementeren. Deze aansprakelijkheid gaat dan over het technische, het organisatorische, het financiële en het juridische. De eigenaar is altijd een directielid met budgetbevoegdheid, die als enige een beslissing kan nemen over de gelopen risico's en hun implicaties op de werking van hun entiteit specifiek en haar rol binnen de Vo in haar geheel. Als er een overlap bestaat tussen verschillende activiteiten of hun processen/ondersteunende infrastructuur, komen de verschillende partijen onderling overeen welke éne persoon de aansprakelijkheid zal dragen. Een typisch profiel hiervoor is een Leidend Ambtenaar of een Administrateur Generaal. Deze persoon mag nooit een extern profiel zijn (bijvoorbeeld consultant).

Een gedelegeerd eigenaar rapporteert rechtstreeks aan een eigenaar en mag in diens naam beslissingen nemen over risico's, budgetten en de werking van de entiteit. Deze verantwoordelijk-heid voor de beheersing van de informatieveiligheidsrisico’s kan een gedelegeerd eigenaar niet nogmaals delegeren naar een lager niveau. Alle beslissingen die de gedelegeerd eigenaar neemt, communiceert hij/zij aan de eigenaar. Een typisch profiel hiervoor is een Afdelings- of Diensthoofd. Deze rol mag niet toegewezen worden aan tijdelijke contracten (bijvoorbeeld consultant), en mag enkel toegewezen worden aan een extern profiel na goedkeuring door een Leidend Ambtenaar of een Administrateur Generaal. Een gedelegeerd eigenaar is verantwoordelijk, maar de eigenaar blijft aansprakelijk.

De uitvoerder is de persoon die het operationele beheer verzorgt. In de praktijk kan dit dezelfde persoon zijn als de (gedelegeerd) eigenaar, hoewel dat niet hoeft. Deze persoon heeft enkel beslissingsrecht over het "hoe", niet over het "wat". Hij/zij bepaalt niet wat er moet gebeuren en heeft enkel de mogelijkheid om een koers te bepalen over hoe dit invulling krijgt. Deze persoon mag een extern profiel zijn (bijvoorbeeld consultant). We hebben volgende uitvoerders geïdentificeerd:

- Een medewerker (werknemers en contractanten tewerk gesteld in opdracht van de Vlaamse overheid) is verantwoordelijk voor het garanderen dat informatie enkel wordt gebruikt in relatie met de opdracht en doelstellingen van de entiteit waarbinnen hij/zij tewerk is gesteld. Enkel en alleen binnen de beperkingen van deze afgelijnde opdracht kan informatie ter beschikking worden gesteld, gewijzigd of verwijderd worden.
- De taken van de functionaris voor gegevensbescherming (FG of DPO) van de entiteit zijn vastgelegd in het Besluit van de Vlaamse Regering betreffende de functionarissen voor gegevensbescherming, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische gegevensverkeer.
- De veiligheidsconsulent/security officer is verantwoordelijk voor de uitvoering van het informatieveiligheidsbeleid.
- De verantwoordelijke voor de IT-dienst adviseert, ondersteunt en voert het informatieveiligheidsbeleid uit.

6. OVERKOEPELENDE AANSTURING EN COORDINATIE

De **Vlaamse Regering** bekrachtigt het informatieveiligheidsbeleid van de Vlaamse Overheid en geeft, overeenkomstig art. 3 laatste lid van het decreet van 23 december 2016 houdende de oprichting van het stuurorgaan Vlaams Informatie- en ICT-beleid, het mandaat aan het Stuurorgaan, om samen met de werkgroep Informatieveiligheid en het agentschap Digitaal Vlaanderen dit informatieveiligheidsbeleid concreet vorm te geven en op te volgen conform de krijtlijnen van deze nota.

De **voorzitter van het Stuurorgaan** voor Informatie -en ICT-beleid is verantwoordelijk voor de validatie van het informatieveiligheidsbeleid voor de Vlaamse administratie[2] en de opvolging van de verwante initiatieven met betrekking tot dreigingen, capaciteitsontwikkeling, rapportering en compliance. Het strategisch plan rond informatieveiligheid maakt integraal deel uit van de strategische agenda van het Stuurorgaan voor Informatie -en ICT-beleid. De leden van dit Stuurorgaan adviseren de voorzitter en koppelen terug naar de eigen entiteit.

De voorzitter van de **werkgroep informatieveiligheid** ondersteunt en adviseert het Stuurorgaan in haar opdracht. De leden van de werkgroep adviseren de voorzitter en het Stuurorgaan en bieden ondersteuning.

De **overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen** zal alle transversale initiatieven coördineren waar een Vo-brede aanpak wenselijk, efficiënter en effectiever is dan een individuele aanpak, uiteraard in verbinding met de entiteit en via het Stuurorgaan en zijn werkgroepen (overleg, inspraak). Hij/zij is verantwoordelijk voor:

- De coördinatie van het Vo-breed strategisch plan met betrekking tot informatieveiligheid, onder meer:
  - het opstellen en onderhoud van het Vo informatieclassificatie raamwerk
- kennisopbouw -en verdeling
- rapportering en afstemming met het Stuurorgaan
- Vo-brede coördinatie met betrekking tot informatieveiligheid (o.m. in geval van kritieke incidenten)

Digitaal Vlaanderen staat eveneens in voor de implementatie van het informatieveiligheidsbeleid en de identificatie en opvolging van risico's binnen de gemeenschappelijke dienstverlening. Digitaal Vlaanderen treedt op als regie-organisatie in directe samenwerking met de strategische stuurgroep van het dienstencentrum ICT. Crisiscoördinatie wordt geformaliseerd in samenwerking met het CCVO.

2 Zoals bepaald in het Bestuursdecreet, zie ook scope van deze nota.

7. RAPPORTERING

De Vlaamse overheid erkent het belang van regelmatige, kwaliteitsvolle en gestandaardiseerde rapportering aan beleidvoerders en beslissingsnemers. Inzicht in de huidige blootstelling op het vlak van risico's bij informatieverwerking binnen de Vlaamse administratie is noodzakelijk om de gepastheid van onze beveiliging te evalueren, zowel op Vo-breed niveau als binnen de individuele entiteiten. Investeringsbeslissingen moeten gebaseerd zijn op actuele en geloofwaardige informatie. Rollen en verantwoordelijkheden moeten hierbij duidelijk opgesteld zijn.

Deze standaardrapportering bevat minstens volgende informatie:

- Een beoordeling (assessment) van de bedreigingen in het kader van informatieveiligheid en de bescherming van persoonsgegevens en de huidige stand van zaken
- Een maturiteitsbeoordeling en gap analyse van de entiteiten
- Opportuniteiten voor samenwerking en Vo beveiligingsdiensten/bouwstenen
- Stand van zaken met betrekking tot investeringen in informatieveiligheid en bescherming van persoonsgegevens.
- Samenvatting van veiligheidsincidenten en gegevenslekken

Om na te gaan of/in hoeverre de entiteit (of een individuele toepassing) voldoet aan het Vo informatieclassificatie raamwerk maken we gebruik van een verplicht self-assessment.

De Vlaamse Regering geeft, overeenkomstig art. 3 laatste lid van het decreet van 23 december 2016 houdende de oprichting van het stuurorgaan Vlaams Informatie- en ICT-beleid, het mandaat aan het Stuurorgaan, om samen met de werkgroep Informatieveiligheid en het agentschap Digitaal Vlaanderen deze standaardrapportering en het proces van self-assessment vast te leggen en op te volgen. Het is de verantwoordelijkheid van de individuele entiteiten om de relevante informatie aan te leveren.

Daarnaast kan een optionele conformiteitstoets worden georganiseerd. Een conformiteitstoets is een proces waarbij gecontroleerd wordt of/in hoeverre de maatregelen genomen binnen een entiteit (of een individuele toepassing) voldoen aan de criteria die beschreven zijn binnen het Vo informatieclassificatie raamwerk. De organisatie zal daarvoor een bewijs ontvangen. Deze kan al dan niet voorwaardelijk zijn, geheel of gedeeltelijk. De conformiteitstoets wordt uitgevoerd door een onafhankelijke partij.

8. PRAKTISCHE VERTALING EN UITVOERING

Deze strategie zal operationeel gemaakt worden door een strategisch plan met een programmastructuur met gepaste middelen, opleiding en training.

De Vlaamse Regering geeft, overeenkomstig art. 3 laatste lid van het decreet van 23 december 2016 houdende de oprichting van het stuurorgaan Vlaams Informatie- en ICT-beleid[5], het mandaat aan het Stuurorgaan, om samen met de werkgroep Informatieveiligheid en het agentschap Digitaal Vlaanderen het strategisch plan vast te leggen en op te volgen.

Het strategisch plan 2021-2024 focust op volgende prioriteiten:

- Een integrale aanpak van informatieveiligheid, als deel van informatiebeheersing
- Verhoogde digitale slagkracht:
    - Door een verhoging van de digitale competenties en
    - Door weerbare processen, geautomatiseerd in robuuste applicaties en infrastructuur

A. VO-BREDE AANPAK VAN INFORMATIEVEILIGHEID

We versterken het leiderschap op het vlak van informatieveiligheid, met inbegrip van bescherming persoonsgegevens door een duidelijk kader, governance en verantwoordelijkheden vast te leggen om tot een Vo gedragen aanpak voor informatieveiligheid te evolueren. Op basis van een periodieke rapportering van hoge kwaliteit moet het voor beslissingsnemers en beleidvoerders mogelijk zijn om de juiste investeringsbeslissingen te nemen.

Met prioriteit A willen we het Vo-brede overzicht en focus op informatieveiligheid leggen:

- Een duidelijk beleidskader binnen de Vlaamse overheid rond het beheersen van risico's op het vlak van informatieveiligheid, met inbegrip bescherming van persoonsgegevens;

- Betere en geïnformeerde beslissingen zowel op Vo-breed niveau als op entiteitsniveau door een duidelijk begrip van de risicoblootstelling van de Vlaamse overheid op het vlak van informatieveiligheid en veiligheid van persoonsgegevens.

B. WE VERHOGEN ONZE DIGITALE COMPETENTIES

Een gebrek aan kennis en expertise met betrekking tot informatieveiligheid leidt tot een situatie waar we niet in staat zijn in te schatten wat de risico's van onze informatieverwerking zijn en ons niet adequaat kunnen beschermen. Op die manier is het onmogelijk onze beoogde doelstellingen te halen.

Met prioriteit B willen we het volgende resultaten bereiken:

- Versterkte slagkracht met betrekking tot informatieveiligheid garanderen door een sterke coördinatie onder toezicht van het Stuurorgaan
- Een breed draagvlak creëren door participatie van diverse stakeholders (werkgroep, private sector, onderzoek, …)
- Capaciteiten verhogen door beroep te doen op strategische partners, gespecialiseerd in cybersecurity
- Minder blootstelling aan risico's met betrekking tot informatieveiligheid door opleiden en bewustmaken van de werknemers van de Vlaamse overheid.
- Interne competentie -en kennisopbouw verhogen door een pool aan specialisten met brede inzetbaarheid.

C. WEERBARE DIGITALE PROCESSEN EN EEN ROBUUSTE INFRASTRUCTUUR

Deze prioriteit heeft als doelstelling om het veiligheidsniveau van de informatieverwerking op operationeel niveau te verhogen door de juiste organisatie en veiligheidsbouwstenen te voorzien. Elke entiteit staat binnen de eigen organisatie in voor het correct implementeren van maatregelen en controles zoals gedefinieerd in de Vo informatieclassificatie van de Vlaamse overheid.

Het is echter logischer en efficiënter om een aantal diensten op een Vo-breed basisaanbod te baseren. Deze zijn onder meer het overkoepelend monitoren en opvolgen van informatieveiligheidsincidenten (operationeel) en het optimaal inrichten van veiligheid gerelateerde dienstverlening (organisatorisch en technologisch). Deze aanpak combineert proactieve en reactieve maatregelen om een zo volledig mogelijke omgeving te bekomen.

Met prioriteit C willen we het volgende resultaten bereiken:

- Verhogen van de maturiteit van onze veiligheidsorganisatie door ondersteuning met betrekking tot veiligheidsdienstverlening & tools
- Geïntegreerde dienstverlening met betrekking tot het beheersen van risico's van onze gemeenschappelijke ICT-systemen
- Verhogen van het operationele veiligheidsniveau door Vo veiligheidsbouwstenen verder uit te bouwen
- Tijdige detectie van informatieveiligheidsincidenten
- Versterkte slagkracht met betrekking tot ernstige informatieveiligheidsincidenten

9. TIMING

Voorliggende strategie gaat van kracht op 1 november 2021.

10. BESTUURLIJKE IMPACT

A. BUDGETTAIRE IMPACT VOOR DE VLAAMSE OVERHEID

Deze nota heeft geen rechtstreeks budgettaire impact voor de Vlaamse overheid. Er worden geen middelen gevraagd. Desalniettemin hange diverse rollen en verantwoordelijkheden aan de uitvoering van deze informatieveiligheidsstrategie die door de bestaande entiteiten moeten worden ingevuld.

De uitvoering van dit beleid zal gebeuren via de reguliere kredieten. Het relance-initiatief "Cybersecurity en uitrol SIEM" (VV065) bevat ook een aantal projecten die betrekking hebben op de praktische vertaling van deze nota.

Het gunstig advies van de Inspectie van Financiën werd op 4/7/2021 verleend (DiVL_I_21_065_KDW_21_551).

Het begrotingsakkoord werd verleend op 11/10/2021.

A. ESR-TOETS

Nihil

11. IMPACT OP HET PERSONEEL VAN DE VLAAMSE OVERHEID

Deze nota heeft geen rechtstreekse impact op het personeel van de Vlaamse overheid. Er worden geen extra VTE gevraagd. Desalniettemin hange diverse rollen en verantwoordelijkheden aan de uitvoering van deze informatieveiligheidsstrategie die door de bestaande entiteiten moeten worden ingevuld.

12. IMPACT OP DE LOKALE EN PROVINCIALE BESTUREN

De scope van de Strategie en het daaruit voortvloeiende informatieveiligheidsbeleid is de Vlaamse administratie zoals bepaald in het bestuursdecreet van 7 december 2018. Waar er uitwisseling van informatie nodig is met andere overheidsinstanties, waaronder de lokale besturen, wordt beroep gedaan op protocollen, zoals voorzien in het e-govdecreet van 18 juli 2008 (decreet betreffende het elektronische bestuurlijke gegevensverkeer).

5. VOORSTEL VAN BESLISSING

De Vlaamse Regering beslist:

1° haar goedkeuring te hechten aan de in deze nota voorgestelde Strategie voor Informatieveiligheid;

2° De Vlaamse minister van Buitenlandse Zaken, Cultuur, Digitalisering en Facilitair Management binnen zijn bevoegdheden te belasten met de opvolging van de verdere uitvoering van de Strategie voor Informatieveiligheid.

De Vlaamse minister van Buitenlandse Zaken, Cultuur, Digitalisering en Facilitair Management

Jan JAMBON

13. BIJLAGE 1: LIJST VAN AFKORTINGEN

ACM	Access Control Management/Beheer van toegangen (authenticatie)
AVG	Algemene Verordening Gegevensbescherming
CCVO	Coördinatie- en Crisiscentrum van de Vlaamse Overheid
DPO/FG	Data Protection Officer/Functionaris gegevensbescherming
LoD	Lines of Defences
PAM	Privileged Access Management/Toezicht op beheer van IT systemen
RACI	Responsible, Accountable, Consultable, Informed/Beschrijvende verdeling van rollen en verantwoordelijkheden binnen de bedrijfsvoering
Vo	Vlaamse overheid