

DE VLAAMSE MINISTER VAN BINNENLAND, STEDEN- EN PLATTELANDSBELEID, SAMENLEVEN,
INTEGRATIE EN INBURGERING. BESTUURSAZAKEN, SOCIALE ECONOMIE EN ZEEVISSERIJ

NOTA AAN DE VLAAMSE REGERING

Betreft: Digitaal Veilig Vlaanderen: Vlaamse beleidsstrategie digitale veiligheid

Samenvatting

Met deze nota legt de Vlaamse Regering de Vlaamse beleidsstrategie digitale veiligheid vast. Met de Vlaamse beleidsstrategie digitale veiligheid zetten we de krijtlijnen uit voor de Vlaamse en lokale overheden. We stemmen strategieën voor overheden, ondernemingen en burgers op elkaar af, aligneren initiatieven en campagnes en stellen onze kennis en instrumenten ter beschikking. Deze centrale aanpak stelt ons in staat om onze maatschappelijke en economische belangen in de online leef- en werkomgeving te beschermen en te bevorderen. Met de beleidsstrategie geven we invulling aan één van de ambities van het Vlaams regeerakkoord en maken we van Vlaanderen de toonaangevende regio van Europa op het vlak van digitale veiligheid.

1. SITUERING

A. BELEIDSVELD/BELEIDSDOELSTELLING

Deze nota kadert in de beleidsvelden Digitalisering, Binnenlands Bestuur, en Steden- en plattelandsbeleid binnen het beleidsdomein Kanselarij, Bestuur, Buitenlandse Zaken en Justitie.

Het dossier speelt in op volgende beleidsdoelstellingen uit het Vlaams Regeerakkoord 2024-2029:

“Vlaanderen maakt werk van een versnelde digitalisering van de overheid en dat in nauwe samenwerking met de lokale besturen. We zetten de werking van het Cyber Response Team voort, zodat Vlaanderen lokale besturen kan bijstaan die te maken krijgen met een acuut cyber risico.” (*Regeerakkoord 2024-2029 p. 203*)

“We streven naar een digitaal veilig Vlaanderen. In het Agentschap Digitaal Vlaanderen creëren we een Vlaams Centrum voor Digitale Veiligheid, waarmee we een sterke veiligheidsstrategie kunnen uitwerken en coördineren in Vlaanderen. We breiden het

////////////////////////////////////

overkoepelende veiligheidsbeleid uit naar de hele Vlaamse overheid en de (boven)lokale besturen. Bij die initiatieven erkennen we bestaande innovaties en waardevolle projecten op lokaal niveau en nemen we hun ervaringen mee.” (*Regeerakkoord 2024-2029*, p. 100 – 101)

De voorgelegde nota kadert eveneens in de **Digitale Strategie voor Vlaanderen** (VR 2025 2706 DOC.0521/1), in het bijzonder speerpunt 6. Digitaal veilig Vlaanderen.

De nota ondersteunt ook de strategische doelstelling SD1 van de Beleidsnota 2024-2029 van het beleidsveld digitalisering: “We realiseren één geïntegreerde digitale strategie voor Vlaanderen in samenwerking met onze interbestuurlijke partners.” De nota legt een duurzaam fundament voor een toekomstbestendige digitale overheid.

B. VORIGE BESLISSINGEN EN ADVIEZEN

- VR 2021 1510 DOC.1151/1 betreffende de strategie voor informatieveiligheid.
- Vlaams Regeerakkoord 2024-2029: Samen werken aan een warm en welvarend Vlaanderen, 30 september 2024.
- VR 2025 0404 DOC.0220/1 betreffende de opstart van het Vlaams Centrum voor Digitale Veiligheid.
- VR 2025 2706 DOC.0521/1 betreffende de digitale strategie voor Vlaanderen.
- VR 2025 1912 DOCXXX betreffende werkplek, netwerk en veiligheidsbouwstenen als norm.
- VR 2026 XXXX DOCXXX Digitaal Veilig Vlaanderen: Vlaams Centrum voor Digitale Veiligheid.

Het Stuurorgaan Vlaams Informatie- en ICT-beleid heeft op haar zitting van 12 februari jongleden kennisgenomen van het dossier. De stukken werden bezorgd en de feedback van de leden werd verwerkt

2. INHOUD

Vlaanderen wil binnen Europa een vooruitstrevende regio zijn, die opportuniteiten uit digitale technologieën en data inzet om maatschappelijke uitdagingen beter aan te pakken en in te spelen op de noden van burgers, ondernemingen en verenigingen. De geopolitieke uitdagingen hebben recent enorm aan belang gewonnen, waardoor Vlaanderen ook voor de uitdaging staat om haar eigen digitale autonomie en digitale veiligheid te waarborgen. De speerpunten en randvoorwaarden voor het garanderen van deze digitale veiligheid worden in de bijlage, nl. de nota Vlaamse beleidsstrategie digitale veiligheid, verder uitgeklaard.

Vlaanderen wil in 2030 een toonaangevende, veerkrachtige, digitaal weerbare en verantwoordelijke regio zijn die in staat is om de Vlaamse belangen in de online leef- en werkomgeving te beschermen en te bevorderen. Een gecoördineerde aanpak is hierbij noodzakelijk. We stemmen de beleidsstrategieën voor de overheden, de ondernemingen en de burgers daarom zoveel als mogelijk op mekaar af, aligneren initiatieven en ondersteuningscampagnes en stellen onze kennis en instrumenten ter beschikking van de Vlaamse en lokale entiteiten alsook de bedrijven. Het Vlaams Centrum voor Digitale Veiligheid (VCDV) speelt hierbij een cruciale rol.

[illegible]

3. VLAAMSE BELEIDSSTRATEGIE DIGITALE VEILIGHEID

We streven naar een veilige digitale leefomgeving. Digitale diensten en openbare dienstverlening in essentiële en kritieke sectoren worden versterkt om het hoofd te kunnen bieden aan de steeds toenemende cyberdreigingen en de toenemende desinformatie. Het VCDV werkt een Vlaamse beleidsstrategie digitale veiligheid en een digitaal veiligheidsbeleid uit en het voert toezicht hierop. Voor de rol en de werking van het VCDV verwijzen we naar volgende beslissingen van de Vlaamse Regering:

- VR 2025 0404 DOC.0220/1 betreffende de opstart van het Vlaams Centrum voor Digitale Veiligheid;
- VR 2026 XXXX DOCXXX Digitaal Veilig Vlaanderen: Vlaams Centrum voor Digitale Veiligheid.

De Vlaamse beleidsstrategie digitale veiligheid heeft tot doel de weerbaarheid tegen cyberdreigingen verder op te bouwen en te versterken en ervoor te zorgen dat:

- de dienstverlening door de Vlaamse overheidsinstellingen en lokale besturen gegarandeerd blijft;
- gevoelige gegevens beschermd worden;
- incidenten zo veel mogelijk voorkomen worden door actief in te zetten op dreigingsanalyses en kwetsbaarhedenbeheer;
- er een strategie voorhanden is om bij incidenten op passende en efficiënte manier te reageren;
- de noodzakelijke veerkracht voorzien wordt om na een incident te herstellen;
- er gebruik gemaakt wordt van betrouwbare digitale technologieën.

Deze centraal gecoördineerde beleidsstrategie garandeert:

- een consistent risicobeheer voor digitale veiligheid;
- een instrumentarium om de verdere digitalisering en de werking in lijn te brengen met het risicobeheer en de wettelijke kaders;
- de centrale opvolging van de risicobeheersing onder meer in verband met het implementeren van de genomen beheersmaatregelen, het uitvoeren van periodieke risicobeoordelingen en de conformiteit met de regelgeving en de beleidsstrategie digitale veiligheid.

Voor de periode 2026-2029 worden er in de beleidsstrategie 7 doelstellingen vooropgesteld (zie bijlage).

[illegible]

4. BESTUURLIJKE IMPACT

A. BUDGETTAIRE IMPACT VOOR DE VLAAMSE OVERHEID

Er is geen financiële impact aangezien het over een doorvertaling van het regeerakkoord gaat. Eventuele bijkomende acties nieuw beleid volgen afzonderlijk het besluitvormingsproces.

De Inspectie van Financiën heeft een gunstig advies gegeven op 5 maart 2026. Met betrekking tot de opmerkingen in het advies worden volgende antwoorden geformuleerd:

- Flankerend beleid:

Het doel van de beleidsstrategie is de weerbaarheid tegen cyberdreigingen van Vlaamse overheidsinstellingen en lokale besturen verder uit te bouwen en te versterken (cfr. Deel 4 speerpunten en doelstellingen). De beleidsstrategie wordt door het VCDV geoperationaliseerd via concrete implementatierichtlijnen. Deze richtlijnen omvatten wettelijke kaders, digitale veiligheidsdoelstellingen en andere verplichte maatregelen of instrumenten zoals een toolbox met templates om een ISMS te implementeren, sjablonen, webinars, trainingen en opleidingen etc. die de toepassing van de beleidsstrategie door Vlaamse overheidsinstellingen en lokale besturen faciliteren. Daar waar reglementair mogelijk is het VCDV-aanbod in principe, mits voorafgaande aanvraag en goedkeuring, beschikbaar voor andere organisaties.

Daarnaast voorziet de beleidsstrategie in een centrale coördinatierol voor het VCDV. Digitale veiligheid is immers een transversale thematiek. Het VCDV zal daarom een geïntegreerd en coherent digitaal veiligheidsbeleid uitwerken en afstemmen tussen de verschillende beleidsdomeinen van de Vlaamse administratie. Het is de bedoeling om regelgevingen, verplichtingen, initiatieven, ondersteuning... inzake digitale veiligheid beter beleidsmatig op mekaar te aligneren, om kennis- en expertisedeling te faciliteren, etc waardoor verschillende doelgroepen nog beter bereikt kunnen worden.

We bekijken hoe het VCDV in het kader van de voorliggende centraal gecoördineerde beleidsstrategie en haar coördinatierol - rekening houdend met bevoegdheden, verantwoordelijkheden en budgettaire contouren – maatschappelijk zo breed mogelijk kan ondersteunen bij het voldoen aan digitale veiligheidsverplichtingen.

- Samenwerking:

Het VCDV onderneemt op dit vlak de nodige stappen. Met het Centrum voor Cybersecurity Belgium (CCB) werd eind 2025 een samenwerkingsovereenkomst rond cyberincidenten en de werking van het Cyber Response Team (CRT) in het Vlaamse Gewest afgesloten. In de ontwerpnota aan de Vlaamse regering betreffende de verdere operationalisering van het VCDV wordt een mandaat gevraagd voor de onderhandeling en ondertekening van een aantal nieuwe samenwerkingsovereenkomsten (o.a. rond het delen van documenten en informatie in het kader van toezicht en rapportering, een 'early warning system' en rond afspraken in het kader van de lopende procedure voor de erkenning als NIS2 sectorale autoriteit gefedereerde overheid). In het voorontwerp van decreet betreft het Vlaamse digitaal veiligheidsbeleid en de oprichting van het VCDV wordt er een delegatie aan het VCDV voorzien om samenwerkingsovereenkomsten af te sluiten met instanties van externe overheden (zoals het CCB, ADiV, e.a.) over de manier waarop het VCDV haar opdrachten uitvoert.

- CCVO:

Wat de beleidsstrategie wel beschrijft is dat het VCVD - in samenspraak met het CCVO - een actieve rol zal opnemen inzake de nodige operationele beveiligingsmaatregelen bij incidenten via het Crisismanagement Team (CMT) CCVO. Ze doet dit gelet op de verwevenheid tussen fysieke en digitale dreigingen en risico's, de nood aan gecoördineerde crisiscommunicatie en de doelstellingen van het VCDV rond crisisafstemming bij ernstige cyberincidenten of aanvallen op strategisch niveau. Deze taak ligt in lijn met de beslissing van de Vlaamse regering rond de oprichting van het VCDV (VR 2025 0404 DOC.0220). Het VCVD doet dit eveneens in het kader van haar SPOC-rol zoals ook bepaald in het Vlaams defensieplan (VR 2025 0404 MED.0119). De concrete afspraken met het CCVO rond verplichtingen en verantwoordelijkheden worden verder vastgelegd.

B. ESR-TOETS

C. IMPACT OP HET PERSONEEL VAN DE VLAAMSE OVERHEID

D. IMPACT OP DE LOKALE EN PROVINCIALE BESTUREN

De bestaande afsprakennota organisatiebeheersing van Audit Vlaanderen - opgesteld in samenwerking met ABB, VVSG, Audio en VVP - wordt aangepast.

Pagina 5 van 6

5. VOORSTEL VAN BESLISSING

De Vlaamse Regering beslist:

1. Haar goedkeuring te hechten aan de in deze nota en bijhorende bijlage voorgestelde Vlaamse beleidsstrategie digitale veiligheid. Deze beslissing vervangt de beslissing van 15 oktober 2021 betreffende de strategie voor informatieveiligheid;
2. De Vlaamse minister van Economie, Innovatie en Industrie, Buitenlandse Zaken, Digitalisering en Facilitair Management te belasten met de opvolging van de verdere uitvoering van de voormelde Vlaamse digitale veiligheidsstrategie.

De minister-president van de Vlaamse Regering, Vlaams minister van Economie, Innovatie en Industrie, Buitenlandse Zaken, Digitalisering en Facilitair Management,

Matthias DIEPENDAELE

De Vlaamse minister van Binnenland, Steden- en Plattelandsbeleid, Samenleven, Integratie en Inburgering, Bestuurszaken, Sociale Economie en Zeevisserij,

Hilde CREVITS

Bijlage: Vlaamse beleidsstrategie digitale veiligheid

////////////////////////////////////