Vlaamse beleidsstrategie digitale veiligheid

1. Context

De Digitale Strategie voor Vlaanderen werd op 27 juni 2025 goedgekeurd (VR 2025 2706 DOC.0521). 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. Via één eenduidige en afgestemde digitale strategie voor de Vlaamse overheidsinstellingen en de andere overheden wordt meer dan ooit ingezet op een datagedreven overheid, op proactieve en slimme diensten, op onze digitale veiligheid en op een inclusieve dienstverlening.

De geopolitieke uitdagingen hebben recent enorm aan belang gewonnen, waardoor Vlaanderen 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 deze nota verder uitgeklaard.

Vlaanderen is in 2030 een toonaangevende, veerkrachtige, digitaal weerbare en verantwoordelijke regio die in staat is om de Vlaamse belangen in de online leef- en werkomgeving te beschermen en te bevorderen.
Vlaanderen is:

- Een veilige en veerkrachtigere regio, voorbereid op evoluerende dreigingen en risico's. We gebruiken onze cybercapaciteiten om burgers, bedrijven en overheden te beschermen tegen beïnvloeding van de publieke opinie op basis van misleidende informatie, digitale dreigingen en misdaad, fraude en staatsdreigingen;
- Een innovatieve, welvarende digitale economie, met kansen die gelijkmatig verspreid zijn over heel de regio en met oog voor digitale inclusiviteit en gelijkheid voor onze diverse bevolking;
- Een pionier op het gebied van wetenschap en technologie, die op veilige en kwalitatieve wijze gebruik maakt van innovatieve en digitale transformaties ter ondersteuning van een inclusieve, veiligere, groenere en democratischere samenleving;
- Een gewaardeerde én betrouwbare partner interbestuurlijk en internationaal, die de toekomstige grenzen van een open en stabiele regio vormgeeft met behoud van onze vrijheid van handelen in de digitale leefwereld.

We streven naar een robuuste digitale veiligheid. We zetten volop in op gekwalificeerd personeel, adequate procedures en instrumentarium en een goede interbestuurlijke samenwerking. Vlaamse en lokale administraties, burgers en ondernemers beschikken over de juiste vaardigheden en tools om zich adequaat te beveiligen in een online en digitale context. We beogen daarom de digitale weerbaarheid in de verschillende lagen van ons sociaal weefsel te versterken.

Vlaanderen werkt een Vlaams digitaal veiligheidsbeleid uit en het voert toezicht hierop. We voorzien een aangepast begeleidings- en ondersteuningsaanbod voor onze Vlaamse en lokale administraties. We verzorgen de opvolging en afhandeling van incidenten via het Vlaams Centrum voor Digitale Veiligheid (hierna het VCDV genoemd). Daarmee bereiken we een robuuste en effectieve digitale veiligheid (VR 20250404 DOC.0220/1BIS).

2. Digitale veiligheid in Vlaanderen

Digitalisering van diensten en technologische toepassingen zijn vandaag niet meer weg te denken in onze samenleving, onze economie en onze overheidsdiensten. Deze digitale en technologische sprong heeft vele voordelen meegebracht, maar we moeten toch ook waakzaam zijn voor risico's en bedreigingen. Cybercriminaliteit is een gegeven waar we constant mee geconfronteerd worden. Er worden immers vaker cyberaanvallen genoteerd en de cybercriminelen gaan hierbij steeds innovatiever te werk. Het aantal veiligheidsincidenten stijgt exponentieel. Digitale veiligheid is essentieel, zowel voor de burger, de overheid als ondernemingen. We zetten samen de krijtlijnen uit om een digitaal veilig Vlaanderen te waarborgen. Een goede interbestuurlijke samenwerking met onder meer het Centrum voor Cybersecurity België (CCB) en met de Algemene Dienst Inlichting en Veiligheid (ADIV) is daarbij cruciaal voor een effectief digitaal veiligheidsbeleid.

De Vlaamse beleidsstrategie digitale veiligheid wil een belangrijke bijdrage leveren in het ontwikkelen van een digitale veiligheidscultuur en de digitale weerbaarheid. We verhogen het bewustzijn, het kennisniveau en de vaardigheden om mogelijke risico's en dreigingen te kunnen waarnemen en adequaat te kunnen reageren. We koppelen hieraan beleidsinitiatieven en maatregelen om onze belangen zo goed mogelijk te vrijwaren.

Beleidsprioriteiten en initiatieven naar de private sector

Het Vlaamse Beleidsplan Cybersecurity werd opgestart in 2019. Op 22 maart 2024 keurde de Vlaamse Regering de tweede cyclus van dit Vlaamse Beleidsplan Cybersecurity goed (VR 2024 2203 DOC.0388). Het beleidsprogramma omvat drie complementaire pijlers:

- (1) Het uitvoeren van top strategisch vraaggedreven basisonderzoek;
- (2) Een centrale focus op de implementatie van cybersecurity-toepassingen in het bedrijfsleven;
- (3) Een sterk flankerend beleid waarin wordt gewerkt aan de significante opleidingsnoden gericht op de arbeidsmarkt.

Om onze Vlaamse KMO's te activeren rond cyberveiligheid bestaat er sinds de start van de cybersecuritybeleidsagenda een gelaagde aanpak via VLAIO met communicatie-acties, kennisverspreiding en opleidingen via collectieve werkvormen zoals lerende netwerken en masterclasses en steun voor individueel gespecialiseerd advies. Zo worden al sinds 2021 cyberveiligheidsverbetertrajecten opgezet. Ze hebben als doel Vlaamse ondernemingen – en in het bijzonder kmo's - te ondersteunen bij het inkopen van extern gespecialiseerd advies om zo op organisatieniveau de cyberveiligheidsmaturiteit te verhogen. De nadruk ligt hierbij voornamelijk op het (proberen) voorkomen van en adequaat reageren op eventuele cyberincidenten.

Via de innovatiesteun bij VLAIO (voor onderzoeks -en ontwikkelingsprojecten) wordt ook ingezet op cyberveiligheid door enerzijds het ondersteunen van Vlaamse ondernemingen die eigen cyberveiligheid-technologie of cyberveiligheid-oplossingen ontwikkelen en anderzijds door ondernemingen die een digitale innovatie willen realiseren te stimuleren van bij de start al voldoende aandacht schenken aan de cyberveiligheidsaspecten. Deze ondernemingen kunnen hiervoor, waar

relevant, ook samenwerken met kennisinstellingen. In de toekomst zullen hier mogelijks ook linken zijn met het impulsprogramma defensie dat in ontwikkeling is.

Omdat onze ondernemingen en overheden met gelijkaardige dreigingen geconfronteerd worden, zoeken we de kruisbestuivingen tussen sectoren op. Door de initiatieven voor de ondernemingen en publieke sector in de toekomst nog meer op elkaar af te stemmen en gemeenschappelijke doelstellingen mee te nemen in het Beleidsplan Cybersecurity, werken we doelmatiger en vergroten we de impact. De uitrol van de cybersecurity beleidsagenda wordt verder opgenomen door VLAIO en het departement WEWIS maar synergiën worden benut. Het VCDV maakt deel uit van de stuurgroep van het Vlaamse Beleidsplan Cybersecurity. Daarnaast zal het VCDV, het departement WEWIS, VLAIO en andere relevante Vlaamse stakeholders periodiek overleggen om beleidsmatig de agenda's te aligneren.

Digitale vaardigheden en competenties

Eén van de pijnpunten is de groeiende kloof tussen de competenties van werknemers en de behoeften van de arbeidsmarkt. De war for talent woedt volop, er zijn ernstige tekorten aan digitale-, STEM-, IT- en datavaardigheden. Binnen het beleidsdomein Werk worden - onder andere door de VDAB - bijkomende initiatieven genomen om de opleidingen te versterken en verbeteren en werkzoekenden beter te wapenen in hun vaardigheden, en ook hun digitale geletterdheid. Het beleidsdomein Onderwijs investeert in een kwaliteitsvol digitaal onderwijs, alsook om de privacy en cyberveiligheid te kunnen garanderen. Beleidsmatig wordt ingezet op ICT-professionalisering van leerkrachten en schoolteams en scholen moeten ook een digitaal veiligheidsbeleid opstellen (Digiplan).

Om capaciteitsnoden rond kennis te borgen, versterkt Vlaanderen het opleidingsaanbod rond digitale veiligheid. We bouwen een laagdrempelig aanbod uit op verschillende niveaus met gedifferentieerde vormingsdoelen (theoretisch versus toegepast). We bekijken eveneens hoe het bestaande aanbod gerichter bekendgemaakt kan worden. Vlaanderen zet hierbij in op drie pijlers:

- Een afdoende basiskennis in het lager en middelbaar onderwijs;
- Afstudeerrichtingen cybersecurity, privacy en informatieveiligheid, waaronder:
  a. technisch gerichte opleidingen op niveau professionele bachelor via hogescholen;
  b. opleidingen op niveau academische bachelor en masteropleidingen;
- Heroriëntatie en bijscholing via onder andere avondonderwijs, VDAB, … en private aanbieders.

In overleg met het departement WEWIS, VLAIO en de betrokken onderzoeksinstellingen zal bekeken worden of er naast het huidige flankerend beleid van het Beleidsplan Cybersecurity een nieuw initiatief kan genomen worden om een soortgelijke werking op te starten gericht op burgers en overheid. We stimuleren samenwerking tussen de onderwijsinstellingen en de opleidingscentra om voldoende coherente en volledige opleidingen aan te bieden zowel aan jongeren als volwassenen. We geven hiermee verder invulling aan het Vlaamse Beleidsplan Cybersecurity en diepen het flankerend beleid uit naar burgers en de overheid, met inbegrip van lokale besturen, onderwijs- en opleidingsinstellingen.

Al in 2023 werd door het Stuurorgaan Vlaams Informatie en ICT-beleid vooropgesteld om ervoor te zorgen dat de Vlaamse bevolking en de VO-medewerkers mee zijn in de steeds versnellende digitale wereld. Met de Digiwijzer van het Agentschap Overheidspersoneel (AgO) wordt de digitale kennis in

kaart gebracht (via de Digistart), waarna er een advies op maat voorgesteld wordt om via e-learnings je digitale vaardigheden op te schalen.

Een uitgebreid flankerend beleid en een eenvormig competentiehandboek versterkt de digitale vaardigheden van overheidspersoneel én burgers. AgO werkt daarom verder samen met het VCDV en andere relevante partners aan een nieuw referentieraamwerk “Digitale Vaardigheden”. Eén overkoepelende, afgestemde en gerichte aanpak zorgt voor meer Vlaamse slagkracht. Op die manier geven we concreet vorm aan een geïntegreerde beleidsstrategie digitale veiligheid voor Vlaanderen.

Vlaams Defensieplan

Het Vlaams Defensieplan (VR 2025 0404 MED.0119) bundelt de acties en beleidsinitiatieven die een stimulans kunnen geven aan de Vlaamse defensiesector. Het is complementair met de inzet voor weerbaarheid, crisismanagement en bescherming van kritieke infrastructuur, zowel binnen de Vlaamse overheid als in interfederaal verband. Eén van de kernpijlers van het plan is inzetten op crisisparaatheid en cyberveiligheid.

De Vlaamse overheid is een volwaardige partner en wordt betrokken bij de opmaak en uitvoering van veiligheids- en weerbaarheidsstrategieën en -plannen (inclusief cyberveiligheid). (Deel 5.1. Vlaams Defensieplan). Het VCDV speelt in het Vlaams Defensieplan een cruciale rol voor het deelluik digitale veiligheid. Het VCDV blijft als aanjager de verschillende werven omtrent digitale veiligheid in het Vlaams Defensieplan opvolgen en aansturen zodat de nodige acties en maatregelen getroffen worden om digitale kwetsbaarheden en bedreigingen te voorkomen, de gevolgen te minimaliseren en digitale weerbaarheid te versterken. Hierbij werken we ook aan de paraatheid van onze digitale én fysieke kritieke infrastructuur zodat we, mits de nodige voorbereidende maatregelen, snel kunnen schakelen bij incidenten en de continuïteit van de dienstverlening kunnen blijven verzekeren of vlug het nodige herstelvermogen kunnen verzekeren.

Het VCDV neemt voor digitale veiligheid de SPOC-rol op voor de Vlaamse entiteiten en lokale besturen richting het Crisiscentrum van de Vlaamse overheid (CCVO), het CCB en de Algemene Dienst Inlichting en Veiligheid (ADIV). Het VCDV gaat in overleg met het CCB en met de inlichtingendiensten Cyber Command en ADIV om tot een nog betere en gecoördineerde samenwerking te komen over de digitale veiligheid (Deel 5.2 Vlaams Defensieplan).

Inclusieve digitale veiligheidsstrategie

De digitale strategie voor Vlaanderen omvat een eenduidige, sterke en afgestemde aanpak over beleidsdomeinen en overheidslagen heen. Eén van de speerpunten is een digitale veiligheidsstrategie die voor iedereen bereikbaar én begrijpelijk is, zodat niemand achterblijft in de digitale omwenteling. Alle Vlamingen moeten gelijke kansen krijgen om deel te nemen aan de digitale wereld. Dit sluit aan op een brede maatschappelijke digitaliseringsagenda. Belangrijke speerpunten in deze strategie zijn digitale veiligheid en het verwerven van digitale vaardigheden en kennis. Zorgen dat iedereen mee is omvat zowel het kaderen van de voordelen als uitdagingen en aandachtspunten van online leefomgevingen en digitalisering.

Het vertrouwen van burgers in de (digitale) overheid staat of valt met een goede beveiliging. Burgers willen zekerheid wanneer hun persoonlijke gegevens gedeeld worden met de overheid. Ze willen zonder zorgen digitale overheidsdiensten gebruiken. Het landschap van cyberdreigingen is in volle

evolutie. Online fraude neemt significant toe en manifesteert zich in verschillende vormen, zoals investerings- of cryptofraude, identiteits-, domicilie- en betaalfraude, nepwebshops, CEO- en factuurfraude, en relatie- of vriendschapsfraude. Ook worden we steeds vaker geconfronteerd met desinformatie en fake news. Het is vaak gericht op het schaden van het vertrouwen in de overheid. We hebben als overheid ook een bewustmakingsopdracht om onze burgers en personeelsleden te wapenen in deze geopolitieke en soms complexe tijden. De Vlaamse overheid en de lokale besturen blijven het eerste aanspreekpunt in het maatschappelijk veld. Een betrouwbare actor zijn is dus een noodzaak.

Om voorop te blijven versterken we ons digitaal veiligheidsbeleid en stellen we een robuuste digitale veiligheid voorop. Het VCDV speelt hierbij een cruciale en centrale rol. Het VCDV zet in op beleidskaders, ondersteuning, opleiding en bewustwording, opdat Vlaamse en lokale besturen beschikken over voldoende kwalitatief geschoolde medewerkers en instrumenten om een correct en objectief digitaal veiligheidsbeleid uit te werken en uit te rollen.

Verder moeten we er ook voor zorgen dat de burgers over de juiste kennis en reflexen beschikken om adequaat en veilig te kunnen ageren in een online context. Op Vlaams niveau wordt door Vlaamse entiteiten, de lokale besturen en partnerorganisaties ingezet op projecten om de digitale weerbaarheid en de inclusiviteit te bevorderen (Digiwijzer, Digibanken, Digiplan, Digitale Inclusie, Veilig Online, …). Steeds meer lokale besturen nemen een digitaal emanciperende rol op en spreken hun inwoners rechtstreeks aan. Ze ontwikkelen een divers aanbod en acties, al of niet samen met partners uit het veld. Denk maar aan de digidokter, infosessies door cyberpreventie-adviseurs, opleidingen in het Lokale Dienstencentrum, mediawijze weken in de bibliotheek, …

Vlaamse economische veiligheidsstrategie

Deze strategie versterkt Vlaanderen in het omgaan met zowel de kansen als de risico's die verbonden zijn aan economische veiligheid in de brede zin. De Vlaamse economische veiligheidsstrategie sluit nauw aan bij het Europese economisch veiligheidskader en bouwt op drie prioritaire actiedomeinen: groei bevorderen, samenwerken en beschermen. Deze aanpak combineert actieve betrokkenheid van het bedrijfsleven en andere stakeholders met gerichte kennisopbouw binnen de Vlaamse overheid. Zo zal de Vlaamse overheid meer aandacht besteden aan het belang van weerbaarheid van economische activiteiten tegen kwaadwillige invloed van autoritaire staten of misbruik voor geopolitieke doelen. Bij het uitwerken van de beleidsstrategie digitale veiligheid en richtlijnen bewaakt het VCDV ook de economische veiligheidsstrategie. We moeten ook zorgen dat de economische activiteiten weerbaar zijn tegen kwaadwillige invloed van onder andere autoritaire staten of misbruik voor geopolitieke doelen. We focussen hierbij onder meer op het waarborgen van de weerbaarheid van toeleveringsketens, fysieke en cyberveiligheid van kritieke infrastructuur; de veiligheid van technologie en het weglekken van technologie en de inzet van economische afhankelijkheid als wapen of economische dwang (dit past binnen het bredere debat over digitale soevereiniteit). In overleg met de departementen Kanselarij en Buitenlandse Zaken en WEWIS worden de beleidslijnen uitgezet.

Het VCDV kan de betrokken administratie ondersteunen in de effectieve toepassing en implementatie van de beleids- en richtlijnen. Specifiek wordt er nauw samengewerkt met het CCVO. Het CCVO coördineert de aanpak van crisissen in samenwerking met de betrokken beleidsdomeinen met respect voor de bevoegdheidsverdeling inzake nationale noodplanning alsook het versterken van

weerbaarheid in de Vlaamse beleidsdomeinen. Het CCVO fungeert als liaison met andere (externe) beleidsdomeinen (federaal, deelstaten, internationaal) en ziet er mee op toe dat de belanghebbende Vlaamse entiteiten door die externe partners betrokken worden.

Weerbaarheid van kritieke dienstverlening en infrastructuur.

De Europese en mondiale crisissen van de afgelopen jaren maakten duidelijk dat een crisisaanpak vanuit elke Vlaamse entiteit afzonderlijk of enkel vanuit de federale noodplanningsactoren niet volstaat. Het samenbrengen van Vlaamse terreinkennis en expertise is noodzakelijk. De voorbereiding en de beleidsmatige gevolgtrekkingen zijn vervlochten met het reguliere beleid. Ook een belangrijk deel van de coördinatie heeft plaats op het Vlaamse niveau.

De CER- en NIS2-richtlijnen versterken de weerbaarheid van essentiële sectoren tegen respectievelijk fysieke en digitale dreigingen in de Europese Unie. De NIS-2 richtlijn is omgezet in een wettelijk kader - de NIS2-wet. De concrete beleidsmatige doorvertaling naar de Vlaamse en lokale besturen gebeurt in het ontwerp van decreet wat betreft het Vlaamse digitale veiligheidsbeleid en de oprichting van een Vlaams Centrum voor Digitale Veiligheid. De omzetting van de Europese richtlijn betreffende de weerbaarheid van kritieke entiteiten (CER) in Belgisch recht gebeurde recentelijk. De wet van 18 december 2025 bepaalt onder meer welke sectoren en deelsectoren onderworpen zijn, wat de identificatie van deze kritieke entiteiten omvat, welke verplichtingen en voorwaarden voor rapportage en informatie-uitwisseling opgelegd worden, en bepaalt de controles en sancties. We gaan na welke maatregelen er in het kader van de richtlijn voor Vlaamse kritieke infrastructuren nodig zijn.

Het VCDV neemt een regierol op voor de koppeling tussen fysieke en digitale veiligheid. In overleg met Het Facilitair Bedrijf en betrokken entiteiten stelt het VCDV de beleidslijnen en richtlijnen op voor de digitale beveiliging van de kritieke infrastructuur. Er is immers een verwevenheid tussen fysieke en digitale dreigingen. Denk onder meer aan fysieke toegangscontrole en toegangsbeheer, fysieke toegang tot gebouwen, datacenters en IT-infrastructuur. De beleidslijnen van het VCDV en de NIS2-referentiekaders omvatten bepalingen om de fysieke risico's en bedreigingen te vermijden of minimaliseren (zie deel 4).

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 neemt het VCVD, in samenspraak met het CCVO, een actieve rol op in het nemen van de nodige operationele beveiligingsmaatregelen bij incidenten via het Crisismanagement Team (CMT) CCVO. Een aanzienlijk aantal Vlaamse en lokale besturen zijn immers actief in kritieke sectoren. Een goede afstemming en gecoördineerde aanpak voor de beheersing van fysieke en digitale incidenten is dan ook aangewezen. Tussen het VCDV en het CCVO worden afspraken vastgelegd rond de voorwaarden voor de escalatie van digitale incidenten en crisissen conform de regionale en nationale noodplannen.

Geïntegreerd Vlaams digitaal veiligheidsbeleid

De bovenstaande opsomming van uitdagingen, initiatieven, regelgeving en plannen toont aan dat er vandaag nog geen geïntegreerd beleid noch een coördinatie of globaal overzicht tussen de verschillende Vlaamse en (boven)lokale beleidslijnen en initiatieven bestaat. Digitale veiligheid raakt menige beleidsuitdaging. Het maximaal kunnen verzekeren van onze (al dan niet kritieke)

dienstverlening moet nagestreefd worden. Denk maar aan onze (zee)havens, het vervoer over de weg en de (binnen)wateren, onze ziekenhuizen en woonzorgcampussen, onze energie- en drinkwatervoorziening, maar ook onder meer de loketdiensten van de gemeenten. Het VCDV neemt hier de coördinerende rol op. Door afstemming te faciliteren met de andere Vlaamse entiteiten, die elk vanuit hun opdrachten rond digitale veiligheid werken, kan een gealigneerd, coherent en geïntegreerd digitaal veiligheidsbeleid ontstaan binnen Vlaanderen. Elke entiteit behoudt de eindverantwoordelijkheid binnen haar eigen bevoegdheidsdomeinen over digitale veiligheid. Op deze manier worden regelgevingen en verplichtingen nog beter beleidsmatig op mekaar gealigneerd, wordt kennis- en expertisedeling gefaciliteerd en worden krachten gebundeld.

Digitale veiligheid is bovenal een complexe maatschappelijke uitdaging die een hoge bestuurlijke en maatschappelijke kost kan hebben. Een adequate beleidscoördinatie is hier op zijn plaats. Het VCDV ontwikkelt een langetermijnvisie en een gecoördineerde aanpak voor digitale veiligheid in Vlaanderen, over alle beleidsdomeinen heen en in samenwerking met alle betrokken doelgroepen (burgers, verenigingen, ondernemingen en overheid). Een holistische aanpak stelt ons in staat om, gelet op de beperkte middelen, de nodige beleidsinitiatieven op te zetten en te anticiperen op toekomstige uitdagingen en kansen. Het biedt ons bovendien de mogelijkheid om uitdagingen en trends vanuit verschillende disciplinaire invalshoeken te bekijken rekening houdend met bredere (geo)politieke, economische en maatschappelijke factoren.

Digitale veiligheid vergt een gezamenlijke aanpak, waarbij elke partner zijn verantwoordelijkheid opneemt. Er moet een risicobewustzijn bestaan en we zorgen dat er de nodige garanties en maatregelen ingebouwd zijn. Het is de taak van het management om ervoor te zorgen dat iedereen zich bewust is van de noodzaak van deze maatregelen[1]. Het “Drielijnenmodel” beschrijft de verschillende rollen en verantwoordelijkheden bij risicobeheersing en monitoring. Dit model geldt ook voor digitale veiligheid en de beheersing van digitale risico’s.

Het identificeren en mitigeren van risico’s is in eerste instantie de verantwoordelijkheid van de entiteit en het management van de organisatie. Dit is de eerste “verdedigingslijn”.

In de tweede “verdedigingslijn” wordt het overkoepelende beleid uitgewerkt en wordt ingezet op kennisverbreding en ondersteuning. Dit gebeurt door de community werking, de ondersteuningstrajecten via opleidingen en webinars, ...

Tenslotte zijn er de formele controle-instanties die toezicht uitvoeren. Dit zijn onder meer het CCB, Audit Vlaanderen, de Vlaamse Toezichtcommissie (VTC), ... Dit is de derde “verdedigingslijn”.

Het toezicht uitgeoefend door het VCDV is geen formele inspectie als controleorgaan. Enerzijds wordt er opgevolgd hoe de Vlaamse overheidsinstellingen en de lokale besturen in overeenstemming zijn met de Vlaamse beleidsstrategie digitale veiligheid. Ook wordt opgevolgd hoe ze ervoor staan rond het nemen van de nodige minimale maatregelen en het NIS2-conform zijn. Anderzijds wordt deze rapportering ook gebruikt om het Vlaams digitaal veiligheidsbeleid en de beleidsondersteuning verder te optimaliseren en waar nodig bij te sturen. Het VCDC fungeert als een strategische facilitator (strategic enabler). Niettemin is afstemming met de formele controleorganen gewenst. Hiervoor is er enerzijds de formele werking van de sectorale overheid met het CCB en anderzijds de afstemming met de formele controle-instanties onder meer via de werkgroep single audit. Met het CCB worden,

[1] In een overheidscontext dus het directiecomité of het managementteam (MAT).

in navolging van de erkenning als sectorale overheid, de samenwerkingsvoorwaarden en afspraken m.b.t. de toezichtrol vastgelegd.

De VTC is de toezichthoudende autoriteit voor de toepassing van de Algemene Verordening Gegevensbescherming (AVG) door de Vlaamse en lokale instanties. Elke verantwoordelijke en elke verwerker van persoonsgegevens is verplicht maatregelen te treffen om een gepast veiligheidsniveau te verzekeren. Het VCDV werkt - na overleg met de VTC - een geactualiseerd en aan NIS2 aangepast kader van minimale beoordelingscriteria van informatieveiligheid uit. Het VCDV doet dit met volle respect voor de autonome en onafhankelijke rol van de VTC als toezichthouder.

3. Digitaal Vlaanderen als de digitale businesspartner voor digitale veiligheid

Digitaal Vlaanderen heeft op basis van het Vlaamse regeerakkoord de opdracht gekregen om de digitale veiligheid binnen de Vlaamse overheid structureel te versterken. Digitaal Vlaanderen heeft de regierol in dit proces en werkt daarbij samen met Vlaamse en lokale overheden en externe partijen. Het VCDV zet het kader en de krijtlijnen uit en de specifieke trajecten en ondersteuningsprojecten geven mee op basis van het beleid de digitale transformaties verder mee vorm.

Digitaal Vlaanderen realiseert dit vandaag enerzijds via een centraal aanbod van werkplek, netwerk en veiligheidsbouwstenen. Het consistent inzetten van de Vlaamse veiligheidsbouwstenen en het gebruik van de centrale werkplek- en netwerkdiensten - met inherente veiligheidsmaatregelen - is een noodzakelijk fundament voor een veilige digitale Vlaamse overheid. Anderzijds worden er specifieke acties opgezet door het aanbieden van platformdiensten, governancemodellen en de expertisecentra interoperabiliteit en AI, ...

In onze dagdagelijkse werking zijn data onmisbaar. Informatie is – samen met de medewerkers - één van de belangrijkste assets voor overheden en bedrijven: zonder data en de daaruit afgeleide informatie is het onmogelijk om processen aan te sturen, beslissingen te nemen of diensten te verlenen. Cybercriminelen zijn zich terdege bewust van de waarde van data en misbruiken die vaak voor kwaadaardige doeleinden. Voorbeelden zijn identiteitsfraude of ransomware-aanvallen waarbij data gegijzeld wordt voor losgeld, zonder enige garantie dat herstel mogelijk is, zelfs na betaling. Dit illustreert dat data niet enkel een bedrijfskritisch hulpmiddel, maar ook een kwetsbaar doelwit vormen.

Om de waarde en veiligheid van data te beschermen, is een goede datahuishouding of data governance cruciaal. Data governance omvat duidelijke afspraken over rollen, verantwoordelijkheden, processen en technologie om data op een betrouwbare, veilige en conforme manier te beheren gedurende de volledige levenscyclus. Digitaal Vlaanderen zet hierbij de krijtlijnen uit voor een goede datahuishouding en zorgt voor ondersteuning bij implementatie.

Ook de verwerking van persoonsgegevens dient zorgvuldig te gebeuren. Burgers moeten erop kunnen vertrouwen dat hun gegevens correct en veilig gebuikt worden en dat er zorgzaam omgesprongen wordt met de bijgehouden data. Als Vlaamse overheid vinden we het van fundamenteel belang dat Vlaamse entiteiten persoonsgegevens altijd verwerken in overeenstemming met de AVG-bepalingen (Algemene Verordening Gegevensbescherming). De hoeveelheid persoonsgegevens, waarover

entiteiten beschikken en die ze verwerken, zijn voor de risico-inschatting van de digitale veiligheid eveneens van belang. Een goede en doordachte dataclassificatie, de inschatting van deze data en informatie op vertrouwelijkheid en integriteit en een goede bepaling van rollen en verantwoordelijkheden zorgt ervoor dat datalekken zo veel als mogelijk voorkomen worden. AVG en digitale veiligheid zijn hierdoor onlosmakelijk met elkaar verbonden. Digitaal Vlaanderen voert voor de Vlaamse bouwstenen en de raamcontracten een overkoepelende Data Protection Impact Analysis (DPIA) uit. Deze referentie-DPIA's worden ter beschikking gesteld en kunnen door de Vlaamse en lokale overheden gebruikt worden in het opzetten van hun veiligheidsstructuur.

Het VCDV zal bij de uitwerking van voorliggende beleidsstrategie digitale veiligheid en de ontwikkeling van het ondersteuningsaanbod richting de doelgroepen niet alleen kijken naar maatregelen op organisatieniveau, maar ook de bescherming van natuurlijke personen en de verwerking van de persoonsgegevens in ogenschouw nemen.

Inbreuken i.v.m. persoonsgegevens die een hoog risico voor de betrokkene inhouden moeten gemeld worden aan de Vlaamse Toezichtcommissie (VTC). We zorgen voor een goede afstemming van de procedures van de verschillende bevoegde instanties wanneer cyberincidenten met inbreuken rond persoonsgegevens zich voordoen.

Het is ook van belang om voldoende aandacht te besteden aan innovatieve technologieën zoals Artificiële Intelligentie (AI). De inzet van AI-bots vergemakkelijkt snelle informatievergaring en stelt organisaties in staat grote hoeveelheden gegevens efficiënt te verwerken. AI speelt ook een cruciale rol bij het verbeteren van digitale veiligheid, onder andere door geavanceerde detectie- en analysemethoden voor dreigingen toe te passen en incidentrespons te ondersteunen. Het Vlaamse digitaal veiligheidsbeleid stelt de inzet van AI als doelgericht en een strategisch instrument ten dienste van digitale veiligheid voorop. Daarnaast bevat het beleid afspraken over veilig gebruik, ontwikkeling en monitoring van slimme toepassingen zoals chatbots. De nadruk ligt op bescherming van persoonsgegevens, toegangsbeheer en toezicht. Het VCDV en het Vlaams veiligheidsbeleid rond AI onderschrijven de principes van de Vlaamse AI-strategie: AI binnen overheden in Vlaanderen is democratisch, betrouwbaar, mensgericht en duurzaam, met correct gebruik en beheer van data en toegepast met kennis van zaken.

Tot slot vormen ook de referentiearchitectuur, de architectuur governance werking en de voorziene uitbreiding van de Vlaamse cloudstrategie de sluitstukken om een veilige IT-structuur te garanderen.

4. Vlaamse Digitale veiligheidsstrategie – Speerpunten en doelstellingen voor de Vlaamse en lokale besturen

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 doel van deze Vlaamse beleidsstrategie digitale veiligheid is 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.

We werken daarom de komende 4 jaar aan de volgende doelstellingen:
1. We beschrijven en coördineren de Vlaamse beleidsstrategie digitale veiligheid vanuit één centraal contactpunt, het Vlaams Centrum voor Digitale Veiligheid.
2. Het VCDV volgt deze beleidsstrategie digitale veiligheid op. De implementatie van de veiligheidsstrategie en implementatie van de NIS2-verplichtingen worden jaarlijks gerapporteerd door de Vlaamse en lokale entiteiten aan het VCDV en gemonitord door het VCDV.
3. We versterken proactief de digitale beveiligingsmaatregelen (Vlaamse bouwstenen, implementatiekader voor risicomanagement voor digitale weerbaarheid en digitale veiligheid, ontwikkeld instrumentarium en tooling).
4. De Vlaamse en lokale overheden blijven verder inzetten om op een veilige wijze de opportuniteiten van digitalisering te verzilveren en gelijktijdig de digitale veiligheid en de publieke waarden te beschermen.
5. Vlaamse en lokale overheden voldoen aan de voorgeschreven veiligheidseisen die voor hen van toepassing zijn.
6. Vlaamse en lokale overheden gebruiken en kopen alleen veilige ICT-producten en diensten.
7. Het VCDV is het regionale CSIRT én centrale aanspreekpunt bij cyberincidenten. De coördinatie, rapportering en opvolging van incidenten gebeurt centraal via het VCDV. De Vlaamse en lokale overheden worden gesensibiliseerd en geoefend in het weren van cyberincidenten en worden hierin door het VCDV ondersteund.

1. We beschrijven en coördineren de Vlaamse beleidsstrategie digitale veiligheid vanuit één centraal contactpunt, het Vlaams Centrum voor Digitale Veiligheid.

Sinds 2021 vormt het 'Informatieclassificatieraamwerk (ICR) 'de leidraad voor informatiebeveiliging' voor alle entiteiten van de Vlaamse administratie (VR 2021 1510 DOC.1151/1). Het ICR wordt ervaren

als een nuttig en tegelijkertijd complex raamwerk. Er is de vraag naar vereenvoudiging en meer concreet toepasbare maatregelen. De Vlaamse administraties zijn reeds jaren aan de slag met het ICR en hebben door hun inspanningen al een positieve maturiteitsgroei doorgemaakt. Deze inspanningen vormen de fundering om verder aan de slag te gaan om de digitale veiligheid te verstevigen. Het ICR wordt meegenomen in het Vlaamse digitale veiligheidsbeleid en wordt verder doorvertaald in implementatierichtlijnen van het Vlaamse digitale veiligheidsbeleid.

Het VCDV is de penhouder van deze Vlaamse beleidsstrategie digitale veiligheid. Eén Vlaams strategisch en operationeel beleidskader zet de krijtlijnen uit voor de Vlaamse overheidsinstellingen en lokale besturen. Deze strategie omvat een geïntegreerde visie en de baselines waaraan Vlaanderen moet en wil voldoen om een digitaal veilige overheid en samenleving na te streven. We zetten de lijnen van deze strategie uit samen met onze partners.

Deze Vlaamse beleidsstrategie digitale veiligheid wordt doorvertaald in implementatierichtlijnen, sjablonen (onder meer de toolbox) en tools (onder meer GRC-tooling, detectieplatformen, ...) om de implementatie door Vlaamse en lokale entiteiten te vergemakkelijken. Het gebruik van het aangereikte instrumentarium brengt deze entiteiten dichter bij naleving van de wettelijke vereisten uit de Belgische NIS2-regelgeving. Het VCDV garandeert de nodige kwaliteit door enerzijds de overkoepelende geïntegreerde aanpak, door de centralisatie van de beleidsvormende en ondersteunende activiteiten en anderzijds door het voorzien van de nodige kennis en competenties in het VCDV en in de partnerdienst Informatieveiligheid van Digitaal Vlaanderen, gelet op de beperkte beschikbaarheid van deze profielen op de arbeidsmarkt. Dit zorgt voor schaalvoordelen en maximale hefbomen zowel op Vlaams als lokaal niveau.
De Vlaamse implementatierichtlijnen bouwen verder op de principes van het ICR en leggen de nadruk op:

- vereenvoudiging van de structuur met verankering van de referentieraamwerken ISO27001 en CyberFundamentals (CyFun®);
- concreet toepasbare maatregelen voor de domeinen waar dit mogelijk is en waar we een gemeenschappelijk basisniveau van beveiliging wensen te hebben;
- ontvlechting van harde eisen en richtlijnen naar praktische handvaten;
- integratie van verplichte maatregelen van het CyFun®raamwerk;
- vereenvoudiging van het risicobeheerproces en het informatieclassificatieschema;
- een eenvoudige set van richtlijnen, templates en maatregelen om het digitaal veiligheidsbeleid en ondersteunende instrumenten te implementeren en ontsluiten.

Het toepassingsgebied wordt stelselmatig uitgebreid naar verschillende overheidsinstantie, zowel op Vlaams als lokaal niveau.

2. **Het VCDV volgt de beleidsstrategie digitale veiligheid op. De implementatie van de veiligheidsstrategie en implementatie van de NIS2-verplichtingen worden jaarlijks gerapporteerd door de Vlaamse en lokale entiteiten aan het VCDV en gemonitord door het VCDV.**

De NIS2-regelgeving vereist dat organisaties tijdig passende organisatorische, operationele en technische maatregelen nemen om risico's te beperken of, als incidenten toch voorvallen, de impact zoveel als mogelijk beperkt of geminimaliseerd wordt. De maatregelen worden bepaald op basis van een risicoanalyse, zoals aangegeven in de ISO27001-norm of de CyberFundamentals (CyFun®). Deze Vlaamse beleidsstrategie bepaalt dat Vlaamse overheidsinstellingen de ISO 27001-norm gebruiken. De lokale besturen hebben de keuze tussen de ISO27001-norm of de CyberFundamentals (CyFun®).

Het implementeren van de nodige maatregelen om cyberincidenten te voorkomen of de gevolgen ervan zoveel mogelijk te beperken is een element van goed bestuur, los van de NIS2-verplichtingen. De Vlaamse beleidsstrategie bepaalt verder dat de Vlaamse overheidsinstellingen en lokale besturen, die niet gevat zijn door de NIS2-reglementering, tegen 1 januari 2030 de nodige maatregelen implementeren om minimaal het zekerheidsniveau 'basis' te behalen. Concreet wil dit dus zeggen dat elke Vlaamse overheidsinstelling of elk lokaal bestuur tegen 1 januari 2030 de minimale maatregelen gekoppeld aan het zekerheidsniveau basis geïmplementeerd heeft. Dit wordt door het VCDV opgevolgd i.k.v. de toezichtsrol die het centrum uitoefent.

Het toezicht van het VCDV is complementair aan de in de NIS2-reglementering voorziene bepalingen rond controle en inspectie. Door een jaarlijkse conformiteitstoets uit te voeren komen de werkpunten naar boven. De ketting is immers zo sterk als de zwakste schakel. Alle administraties hebben er baat bij dat de digitale weerbaarheid zo optimaal mogelijk is gelet op de sterke verbondenheid van de verschillende overheidsdiensten. Verder geeft deze jaarlijkse meting een beeld waar het beleid nog aangescherpt kan worden, zodat de nodige ondersteuningstrajecten voorzien kunnen worden.

Het VCDV volgt het behalen van de vooropgestelde rapporteringsmijlpalen op en ondersteunt de Vlaamse overheidsinstellingen en lokale besturen hierbij.
In 2026 volgt een eerste rapporteringsmijlpaal. De doorvertaling van het beleid binnen de Vlaamse overheidsinstellingen en lokale besturen wordt in een eerste fase opgevolgd door de analyse van de verklaringen van toepasselijkheid en de verificaties die door erkende conformiteitsbeoordelingsinstanties (CAB's) worden uitgereikt.
Vanaf 2027 volgt het VCDV jaarlijks de toepassing van het Vlaams digitaal veiligheidsbeleid, de implementatie van de nodige beheersmaatregelen en het zich confirmeren aan het vooropgestelde zekerheidsniveau op bij de Vlaamse en lokale entiteiten. Dit beleidstoezicht gebeurt door het analyseren van de aangeleverde rapporten. De rapporten worden opgemaakt op basis van richtlijnen die het VCDV opstelt. Het VCDV zal er maximaal op toezien dat de rapportering geen bijkomende planlast veroorzaakt. Elke entiteit ontvangt een overzichtsverslag na de analyse.

Het VCDV bezorgt jaarlijks geaggregeerd en geanonimiseerd het compliancerapport aan het Stuurorgaan Vlaams Informatie- en ICT-beleid, het Auditcomité van de lokale besturen, het auditcomité van de Vlaamse administratie en Audit Vlaanderen.

Wanneer het VCDV vaststelt dat een Vlaamse overheidsinstelling of een lokaal bestuur niet voldoet aan de jaarlijkse rapporteringsverplichting of de verplichting tot het uitvoeren van een driejaarlijkse conformiteitsbeoordeling (zie doelstelling 3 hieronder), kan het een administratieve sanctie opleggen. Het voorzien van deze maatregel beoogt een preventief effect om de overheidsinstellingen en lokale besturen maximaal aan te zetten om aan de verplichtingen te voldoen.

3. **We versterken proactief de digitale beveiligingsmaatregelen (Vlaamse bouwstenen, implementatiekader voor risicomanagement voor digitale weerbaarheid en digitale veiligheid, ontwikkeld instrumentarium en tooling).**

De Vlaamse beleidsstrategie digitale veiligheid is leidend voor het versterken en 'onderhouden' van de Vlaamse en lokale digitale veiligheidsstrategie. De Vlaamse beleidsstrategie digitale veiligheid wordt doorvertaald in implementatiemaatregelen, digitale veiligheidsdoelstellingen en digitale veiligheidsrichtlijnen. Deze implementatiemaatregelen beschrijven hoe de minimale maatregelen, die vanuit wet- en regelgeving of veiligheidsadviezen worden vereist m.b.t. de verwerkingen en beveiliging van informatie, concreet doorvertaald moeten worden. Ze verduidelijken verder ook de verplichtingen die nodig zijn om te voldoen aan de conformiteitsbeoordelingsraamwerken ISO27001 en/of CyFun®. Hierna volgen een aantal voorbeelden.

Om de implementatie van deze Vlaamse beleidsstrategie te ondersteunen, kan het VCDV gebruiksvriendelijke instrumenten, zoals de Toolbox "Digitale Veiligheid: Ondersteuning" en een "Governance, Risk and Compliance" (GRC) -tool, ter beschikking stellen aan de besturen.

Het VCDV ondersteunt de Vlaamse en lokale besturen ook met een aanbod dat zich richt op de menselijke component van beveiliging, met onder meer opleidingsmodules, een trainingsaanbod en bewustwordingscampagnes, maar ook de doorvertaling naar formele contractuele en arbeidsrechtelijke clausules, richtlijnen en andere formele kaders.

Om kwalitatieve digitale diensten te voorzien worden de Vlaamse bouwstenen verder geïmplementeerd. We streven altijd naar de sterkste authenticatie en identificatie standaarden. Het VCDV beschrijft de authenticatieprocedures en mogelijke authenticatie technologieën. Sterke authenticatie houdt onder meer multifactor authenticatie, de implementatie van de Vlaamse bouwsteen ACM/IDM of gelijkwaardige oplossingen. Ook wordt verder ingezet op een goede cyberhygiëne door bijvoorbeeld toepassing van het least privilige principe en een doorgedreven accountbeheer en -review. Daarnaast is er ook aandacht voor het definiëren van een effectief paswoordenbeleid.

Om de besturen te ontzorgen worden centraal en op maat kwaliteitsvolle veiligheidsdiensten aangeboden zoals kwetsbaarhedenrapportering, pentesting,...Het VCDV zet actief in op het vroegtijdig detecteren van kwetsbaarheden en bedreigingen. Deze radarfunctie vormt één van de steunpijlers van deze Vlaamse beleidsstrategie. Door actief in te zetten op het screenen van potentiële dreigingen en anomalieën wordt de effectieve impact van een incident voorkomen en blijft het vertrouwen in de overheid gegarandeerd.

Het VCDV is ook de centrale spil om alle meldingen via de Security Operations Centers (SOC's) op te volgen en analyseren. De informatie van de (Vlaamse) SOC, die centraal door Digitaal Vlaanderen aan de entiteiten aangeboden wordt, wordt verder aangevuld met de data die gegenereerd worden door de SOC's, die de lokale besturen of Vlaamse overheidsinstellingen inzetten. Om de mazen van het net klein en de blik scherp te houden stelt het VCDV voorop dat deze besturen met een eigen SOC

moeten garanderen dat hun diensten minimaal voldoen aan de voorwaarden van de Vlaamse SOC zoals voorzien binnen de centrale dienstverlening van Digitaal Vlaanderen. Het toezicht hierop wordt ook meegenomen in de jaarlijks aan te leveren rapportering door de betrokken entiteiten.

Digitaal Vlaanderen biedt verder ook centrale dienstverlening aan om aan systeem- en securitymonitoring te doen. Naast de monitoring van dreigingen en de identificatie van incidenten door het security operations center (SOC), wordt ook een breed pallet van security monitoringsystemen aangeboden (onder meer SIEM, SOAR, EDR, XRD, …). Het opvolgen van kwetsbaarheden en dreigingen is een belangrijke prioriteit van het VCDV en bij uitbreiding van de Vlaamse en lokale besturen. Door het aanbieden en actief aanmoedigen van de diensten van van ethische hackplatformen en phishingplatformen[2] verscherpen we onze blik. Het gebruik van deze centrale dienstverlening wordt aangemoedigd. Het comply or explain-principe wordt in de jaarlijkse rapportering meegenomen met betrekking tot het al dan niet gebruik maken van deze centrale dienstverlening.

Entiteiten die gedeeltelijk, afwijkend of niet geïntegreerd zijn met de centrale dienstverlening inzake digitale veiligheid vanuit Digitaal Vlaanderen, dienen zelf in te staan voor het realiseren van een veilige werkomgeving. Deze entiteiten moeten een evenwaardig niveau als de dienstverlening van Digitaal Vlaanderen garanderen zodat de beveiliging op het niveau van de Vlaamse overheid consistent is. Deze entiteiten moeten zich conform stellen aan het digitale veiligheidsbeleid van de Vlaamse overheid. Indien het VCDV vaststelt dat een Vlaamse overheidsinstelling of een lokaal bestuur ernstige tekortkomingen vertoont met betrekking tot de naleving van de Vlaamse beleidsstrategie digitale veiligheid en de implementatierichtlijnen of de NIS2-regelgeving, en daardoor de digitale veiligheid van andere Vlaamse overheidsinstellingen of lokale besturen in gevaar brengt, kan de toegang tot de centrale dienstverlening van het agentschap Digitaal Vlaanderen geheel of gedeeltelijk ontzegd worden.

Om erop toe te zien dat het Vlaams digitaal veiligheidsbeleid en de implementatierichtlijnen correct geïmplementeerd worden, moeten entiteiten die geen verplichte certificering in het kader van NIS-2 hebben uitgevoerd, periodiek (3-jaarlijks) een conformiteitsbeoordeling door een onafhankelijke partij laten uitvoeren. Bij de verificatie daarvan wordt de implementatie van specifieke (technische) maatregelen en hun overeenstemming met het volgens de Vlaamse beleidsstrategie digitale veiligheid of NIS2-regelgeving te behalen zekerheidsniveau nagegaan. Voor entiteiten die zich vrijwillig hebben laten certificeren in het kader van NIS-2 zal deze conformiteitsbeoordeling gebruikt worden. De uitkomst van de verificatie maakt onderdeel uit van de digitale rapportering die onder doelstelling 2 aangereikt wordt.

[2] SOC: Security Operations Center; SIEM: Security Information and Event Management; SOAR: Security Orchestration, Automation, and Response ; EDR: Endpoint Detection and Response; XRD: Extended Detection and Response.

4. **De Vlaamse en lokale overheden blijven verder inzetten om op een veilige wijze de opportuniteiten van digitalisering te verzilveren en gelijktijdig de digitale veiligheid en de publieke waarden te beschermen.**

De overheid heeft de maatschappelijke taak om op een correcte en veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en tegelijkertijd de digitale veiligheid en publieke waarden te beschermen. Als onderdeel van deze brede maatschappelijke opgave heeft de overheid de taak het goede voorbeeld te geven en op een veilige manier met gegevens van burgers om te gaan.

Het VCDV en de Vlaamse en lokale ecosystemen zetten volop in om het bewustzijn bij de besturen te verhogen door (centrale) sensibiliseringscampagnes, trainingen en webinars aan te bieden. Ook het periodiek uitvoeren van de risicoanalyses versterkt onze weerbaarheid tegen potentiële dreigingen. Het VCDV zal overheidsbrede crisisoefeningen (mee) faciliteren. Er wordt ook ingezet op het verder versterken van proactieve beveiligingsmaatregelen zodat de belangen en kerntaken van de Vlaamse en lokale besturen zo veel als mogelijk gegarandeerd kunnen worden of dat de risico's bij incidenten zo veel mogelijk beperkt worden.

De Vlaamse en lokale besturen zetten in op aangepaste training en opleidingen voor de 'bestuursorganen' en de personeelsleden rond digitale veiligheid. Kennis over de NIS2-regelgeving, digitale veiligheid en digitale vaardigheden zijn vandaag een noodzakelijke voorwaarden. De (C)ISO-rol speelt vandaag en ook de volgende jaren een belangrijke rol in de dagdagelijkse werking van onze entiteiten. De (C)ISO heeft een adviserende rol en verantwoordelijk voor het informatiebeveiligingsbeleid, risicobeheer en de bescherming van de bedrijfsinformatie. De Vlaamse overheidsinstellingen en lokale besturen wijzen een functionaris voor digitale veiligheid aan. Het aanstellen van deze (C)ISO zit vervat in de referentieraamwerken ISO27001 en CyFun®. De (C)SIO moet over een duidelijk mandaat en voldoende middelen beschikken.

5. **Vlaamse en lokale overheden voldoen aan de voorgeschreven veiligheidseisen die voor hen van toepassing zijn.**

Naast de beleidslijnen vermeld onder doelstelling 3 worden in de "Toolbox" ook sjablonen gepubliceerd die toelaten om een beheersysteem voor informatieveiligheid (ISMS) op te zetten. Door systematisch de digitale veiligheid te waarborgen en te verbeteren wordt de conformiteit met ISO27001 en/of CyFun® gefaciliteerd. In de "Toolbox" wordt de koppeling gemaakt met de Vlaamse bouwstenen en de door Digitaal Vlaanderen aangeboden raamcontracten, zodat de NIS2-conformiteit van de toeleveringsketen ook gegarandeerd is.

Bij uitbesteding van ICT-dienstverlening en aankopen van ICT-diensten en -producten moet er immers rekening worden gehouden met specifieke kwetsbaarheden of risico's bij de leverancier of ICT-dienstverlener. Er moet worden nagegaan welke vereisten gesteld moeten worden aan de leverancier of dienstverlener en de specifieke ICT-producten. Deze ICT-producten en ICT-diensten moeten eveneens de "digitaal veilig"-toets doorstaan. Dit is ook gekend als cyberbeveiliging in de toeleveringsketen of supply chain met de rechtstreekse leveranciers of dienstverleners. Voor ICT-

diensten of -producten die afgenomen worden via de ICT-raamcontracten of de product- en dienstencataloog van Digitaal Vlaanderen zijn de basisvoorwaarden voor cyberbeveiliging gegarandeerd. Specifieke hogere cyberbeveiligingsgaranties moeten door de individuele entiteit met de respectievelijke leverancier of dienstverlener opgenomen worden.

Overheden beheren veel gevoelige data. Het is essentieel om kaders te creëren die garanderen dat deze gegevens ook in de toekomst veilig worden opgeslagen en versleuteld. Een actuele dreiging is het “harvest now, decrypt later”-scenario: hierbij worden nu versleutelde gegevens onderschept en opgeslagen, met de bedoeling ze later – wanneer de technologie het toelaat – te ontsleutelen. Organisaties die gevoelige informatie langdurig geheim moeten houden, krijgen daarom het advies om zich nu al te wapenen tegen toekomstige quantumdreigingen, zoals:

- het ondermijnen van de integriteit van digitale handtekeningen;
- het aantasten van de betrouwbaarheid en integriteit van gegevens en systemen.

We blijven inzetten op baanbrekende en innovatieve technologieën. AI-bots stellen ons in staat om snel informatie te vinden en efficiënt omvangrijke datasets te analyseren. Om goed te functioneren, om hun modellen te trainen en bias uit te sluiten, is een duidelijke beschrijving nodig van de vereisten waaraan de dataset moet voldoen. Met een correct gebruik en beheer van data en een toepassing van AI met kennis van zaken, kan AI gebruikt worden om de digitale veiligheid te optimaliseren. Door toepassing van dataclassificatie kan data correct gelabeld worden volgens gevoeligheid. Hierdoor kunnen technische maatregelen zoals toegangsbeperkingen en encryptie doelgericht toegepast worden. We bewaken dat AI-chatbots of andere technologische systemen geen ongecontroleerde toegang krijgen tot overheidsinformatie.

Het VCDV stelt een AI-veiligheidsbeleid op alsook een beleid rond het toepassen van encryptie, quantum en postquantum. Het AI-veiligheidsbeleid beschrijft de principes en richtlijnen voor het ethische, veilige en doeltreffende gebruik van AI-technologieën. Het heeft als doel de krijtlijnen uit te zetten die ervoor te zorgen dat AI op verantwoorde wijze wordt ingezet ter bevordering van productiviteit, innovatie en besluitvorming, terwijl risico’s worden geminimaliseerd en de waarden van het VCDV én de Vlaamse administraties en lokale besturen worden beschermd. Dit AI-veiligheidsbeleid bevat richtlijnen voor het gebruik, de ontwikkeling en het toezicht op generatieve AI-toepassingen, zoals chatbots die werken met Large Language Models (LLM’s). Hierbij wordt bijzondere aandacht besteed aan gegevensbeveiliging, toegangscontrole en monitoring. Het beleid beschermt gevoelige data, voorkomt misbruik en waarborgt naleving van wet- en regelgeving zoals de AVG en EU AI Act. Door het risico op datalekken te beperken, kunnen we het vertrouwen van hun burgers, leveranciers en partners behouden. De overgang naar postquantum en homogene encryptie zal grote gevolgen hebben voor bestaande systemen en de manier waarop gegevensbeveiliging wordt georganiseerd. In een snel veranderend technologisch landschap is het daarom van strategisch belang om internationale ontwikkelingen nauwgezet te volgen en tijdig het digitaal veiligheidsbeleid en de technische implementaties aan te passen. Alleen zo blijft de digitale veiligheid gewaarborgd.

6. Vlaamse en lokale overheden gebruiken en kopen alleen veilige ICT-producten en diensten (incl. minimale vereisten voor eigen ontwikkeling)

Veilige ICT-producten en -diensten aankopen of ontwikkelen is een vanzelfsprekendheid. Het VCDV zet de richtlijnen uit waaraan producten, diensten en dienstenleveranciers moeten voldoen om deze

doelstelling te realiseren. Digitaal Vlaanderen en de geprivilegieerde externe partners leveren oplossingen aan die voldoen aan de vooropgestelde wettelijke en technologische eisen.

Digitaal Vlaanderen zorgt voor een gedragen, gestandaardiseerde en veilige infrastructuur en toepassingen door:

- Referentiearchitectuur te ontwikkelen en de toepassing ervan op te volgen;
- Beleidsrichtlijnen, blue prints en adviezen op te stellen om veilige diensten en toepassingen te ontwikkelen of aan te kopen;
- Gemeenschappelijke diensten en bouwstenen aan te bieden (al dan niet via de geprivilegieerde externe partners en de raamcontracten).

Digitaal Vlaanderen realiseert vandaag al veilige oplossingen via een centraal aanbod van werkplek, netwerk en veiligheidsbouwstenen. De adoptiegraad van dit centraal aanbod is goed, maar behelst nog niet alle Vlaamse overheidsadministraties. Concreet ligt de focus op:

1. De werkplek omdat dit één van de primaire ingangspoorten voor cyberaanvallen is. Het VCDV stelt voorop dat de werkplekken maximaal digitaal aangeboden worden;
2. Het netwerk als cruciale sensor voor het detecteren van cyberaanvallen. Digitaal Vlaanderen implementeert op korte termijn het Generieke Infrastructuur Diensten (GID)-netwerk, waarbij een gestandaardiseerde, veilige en schaalbare netwerkconnectiviteit gerealiseerd wordt. 24/7 monitoring wordt voorzien zodat incidenten proactief gedetecteerd en opgelost worden;
3. De verdere – verplichte – uitrol van de veiligheidsbouwstenen. Dit biedt een consistente en geverifieerde toegang tot alle diensten.

Het consistent inzetten van de veiligheidsbouwstenen en het gebruik van "werkplek- en netwerk als norm” - met inherente veiligheidsmaatregelen - is immers een noodzakelijk fundament voor een veilige digitale Vlaamse overheid. Deze drie doelstellingen worden zoveel als mogelijk doorvertaald naar het lokale overheidslandschap. Deze gemeenschappelijke aanpak:

- Resulteert in een verhoogde digitale weerbaarheid/veiligheid van de overheidsadministraties;
- Zorgt voor de nodige compliance met de Vlaamse beleidsstrategie digitale veiligheid en de NIS2-verplichtingen;
- Beoogt efficiëntiewinsten en zorgt voor schaalvoordelen.

Door centralisatie en standaardisatie van infrastructuur en beveiliging wordt de weerbaarheid tegen digitale risico’s verhoogd, de naleving van de regelgeving vereenvoudigd en de gebruikerservaring verbeterd. Ook hier wordt het comply or explain principe toegepast. De administraties zijn verplicht te bevestigen dat ze de beleidslijnen en regels naleven (comply) of, als dat niet het geval is – namelijk bij gedeeltelijke, afwijkende of geen integratie - duidelijk uitleggen waarom ze afwijken (explain).

7. **Het VCDV is het regionale CSIRT én centrale aanspreekpunt bij cyberincidenten. De coördinatie, rapportering en opvolging van incidenten gebeurt centraal via het VCDV. De Vlaamse en lokale overheden worden gesensibiliseerd en geoefend in het weren van cyberincidenten en worden hierin door het VCDV ondersteund.**

Het VCDV blijft inzetten op de ondersteuning en ontzorging van de Vlaamse en lokale instanties bij cyberincidenten. Dit deelluik wordt opgenomen door het regionaal Computer Security Incident

Response Team (CSIRT). Het regionale CSIRT fungeert als centraal aanspreek- en coördinatiepunt voor cyberincidenten met impact op de Vlaamse en lokale besturen. Om dit op een effectieve wijze te realiseren wordt ingezet op meerdere actiepunten, zowel proactief als reactief.

Door acute dreigingsinformatie te centraliseren, vanuit de Vlaamse overheid, de lokale besturen én vanuit de partners (CCB,...) en toeleveranciers, en proactief te communiceren over (risico tot) incidenten kunnen we zorgen voor een veiligere overheid.
Sensibilisering en bredere kennisdeling binnen het netwerk zorgen ervoor dat het VCDV sneller kan reageren. Door een actieve samenwerking en kennisdeling tussen de verschillende overheden kan sneller geageerd worden om incidenten te voorkomen of de impact zo beperkt mogelijk te houden.

Bij een incident is het belangrijk dat de geïmpacteerde entiteit gemakkelijk geïdentificeerd en gecontacteerd kan worden. Dit impliceert het kunnen beschikken over een centraal overzicht van de ICT-assets. Het VCDV coördineert de opmaak van dit centraal overzicht én is centraal contactpunt. Wanneer er zich incidenten voordoen bij de Vlaamse overheidsinstellingen en lokale besturen - die tot het toepassingsgebied horen - zal het CSIRT-team adviesverlening en ondersteuning bieden. In eerste fase assisteert het team bij de opvolging van de wettelijke verplichtingen zoals de initiële en tussentijdse rapporteringen bij het CCB.

Meldingen van onregelmatigheden of incidenten gebeuren centraal aan het regionale CSIRT. Het CSIRT zal de evaluatie maken of een incident als een cyberincident gekwalificeerd wordt of niet. Niet enkel cybersecurityincidenten maar ook langdurige onderbrekingen moeten immers aan het CCB gemeld worden en bij operationele onderbrekingen moet ook nagegaan worden of er bijkomend geen andere indicaties voorhanden zijn. Het regionaal CSIRT zal samen met de entiteit de verplichte rapportering aan het CCB verzorgen[3.]

Het Vlaamse CSIRT-team beschikt over technische expertise op vlak van forensisch onderzoek. Hierdoor kan men gerichte ondersteuning bieden bij de getroffen entiteiten om de grondoorzaak bij incidenten te bepalen en bredere impact te voorkomen.
Verder helpt het Vlaamse CSIRT-team bij de coördinatie bij het beheersen van incidenten. De partners krijgen gericht advies en hebben ondersteuning waar nodig om de prioriteiten op het technische en strategische niveau op elkaar af te stemmen. Indien nodig kan het VCDV de escalatie opstarten volgens de regionale en nationale noodplannen. Er worden hieromtrent afspraken gemaakt met het CCVO (zie ook hoofdstuk 2).

Met de Vlaamse overheidsinstellingen en lokale besturen die momenteel al een eigen incident response hebben, worden werkafspraken gemaakt om de informatiedoorstroming te stroomlijnen, zodat de incidenten centraal opgevolgd kunnen worden De instanties met een eigen incident response moeten minimaal voldoen aan de voorwaarden rond kwaliteit, prestaties en responstijden zoals deze voorzien zijn bij het regionale CSIRT van het VCDV. Het toezicht hierop wordt meegenomen in de jaarlijkse rapportering van de betrokken entiteiten.
Remediëring en ontzorging bij incidenten is noodzakelijk. Maar voorkomen is beter. Daarom blijft het VCDV volop inzetten om voorafgaand kwetsbaarheden en bedreigingen te detecteren. Door de

[3] art. 34 en art. 35 van de NIS2-wet.

radarfunctie verder uit te bouwen en volop in te zetten op preventieve scanning trachten we zo veel als mogelijk incidenten te voorkomen (zie ook doelstelling 3).

5. Vlaams Centrum voor Digitale Veiligheid

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 0403 DOCXXX Digitaal Veilig Vlaanderen: Vlaams Centrum voor Digitale Veiligheid.