stichting
VO Haaglanden

Informatiebeveiliging en privacy strategie

2024 - 2028

versie 1.6

19-01-2024

Parkstraat 83
2514 JG Den Haag

info@vohaaglanden.nl
www.vohaaglanden.nl

T (070) 426 26 26

stichting
VO Haaglanden

stichting
VO Haaglanden

Inleiding

Informatiebeveiliging en Privacy is geen opzichzelfstaand onderwerp. Het draagt bij aan een veilige leer- en werkomgeving en sluit daarmee aan op een groot aantal strategische uitgangspunten genoemd in het *Strategisch plan 2021-2025*[1] en aan de maatschappelijke opdracht van VO Haaglanden.

Onze organisatie werkt veel met waardevolle en vertrouwelijke informatie en met de voortdurende ontwikkelingen op digitaal gebied is Informatiebeveiliging en Privacy een breed en complex onderwerp geworden. Het werken vanuit een visie en strategische uitgangspunten voor Informatiebeveiliging en Privacy is daarom noodzakelijk om aantoonbaar te groeien naar een professionele en veilige manier van omgaan met de beschikbaar gestelde informatie.

Dit document geeft binnen de context van de door VO Haaglanden benoemde strategische richting een basis om concreet en planmatig aan de slag te gaan met onze Informatiebeveiliging en Privacy in het bijzonder.

Informatiebeveiliging en Privacy

Informatiebeveiliging en Privacy staat voor beveiliging van waardevolle informatie (Security) en bescherming van persoonsgegevens (Privacy). VO Haaglanden draagt hierin een grote verantwoordelijkheid. Beschikbaarheid, Integriteit en Vertrouwelijkheid van de informatie zijn kernbegrippen.
Informatiebeveiliging en Privacy is essentieel voor:

1. De continuïteit van het onderwijsproces;
2. Kwalitatief hoogwaardig onderwijs;
3. Een veilige leer- en werkomgeving.

Informatiebeveiliging en Privacy is geen doel op zich maar draagt bij aan de volgende strategische uitgangspunten van VO Haaglanden:

1. Toekomstbestendig pluriform onderwijs
2. Kennisdeling en samenwerking
3. Professionele (onderwijs)organisatie;
4. Intrinsieke leer- en verbetercultuur;
5. Een sterke organisatie.

Missie en maatschappelijke opdracht

De VO Haaglanden strategie levert een bijdrage aan de missie en de maatschappelijke opdracht. Het nemen van de verantwoordelijkheid om samen met de schoolleiders zorg te dragen voor een stelsel van onderwijsvoorzieningen in Den Haag en Rijswijk, dat alle jonge mensen - in samenwerking met de ouders - ondersteuning biedt die past bij hun aanleg en ambitie. We doen dat door het in stand houden en stimuleren van een pluriform scholenbestand. Onze scholen zijn openbaar of algemeen bijzonder. De scholen richten zich op een grote verscheidenheid van doelgroepen, waarbij het tegengaan van kansenongelijkheid een belangrijke opdracht is. Dit is ook terug te vinden in onze kernwaarden; pluriform en eerlijke kansen, gericht op ontwikkelen, solidair en samen, vertrouwen en persoonlijk.

[1] https://www.vohaaglanden.nl/public/Download/16/bestand/Strategisch%20plan.pdf

Visie in relatie tot Informatiebeveiliging en Privacy

VO Haaglanden wil een veilige en professionele leer- en werkomgeving aanbieden en daarbij is het noodzakelijk dat de door VO Haaglanden verzamelde, verwerkte en gepubliceerde informatie te allen tijde beschikbaar, correct en beschermd is. Dit vraagt om een strategisch samenhangende aanpak van Informatiebeveiliging en Privacy, die aantoonbaar aan de eisen voldoet, om blijvend een veilige en toekomstbestendige leer- en werkomgeving beschikbaar te stellen.

De uitvoering van deze visie maken we concreet doordat we de richtlijnen zoals vastgelegd in het *Digitaal Funderend Onderwijs 2023* gaan implementeren en naleven.

Strategie

Met als basis het *Strategisch plan 2021-2025*, waarin o.a. benoemd pluriformiteit, hoge kwaliteit, bereikbaarheid, eigenheid en ontwikkelingskansen, rekening houdend met onze maatschappelijke opdracht en kernwaarden wil VO Haaglanden groeien naar een professionele organisatie, op het gebied van informatiebeveiliging en privacy, waar op een veilige manier onderwijs verzorgd en ondersteund kan worden.

In aansluiting hierop willen we met een strategische aanpak op het gebied van Informatiebeveiliging en Privacy groeien naar een professioneel volwassen organisatie, waar op een veilige manier met informatie wordt omgegaan.

Deze strategie is richtinggevend en sluit aan bij de bovengenoemde uitgangspunten van VO Haaglanden, genoemd in het *Strategisch plan 2021-2025*[2].

We verbinden verschillende aandachtsgebieden op het gebied van informatiebeveiliging en privacy, vanuit één strategische visie. Door jaarlijks te evalueren blijven we flexibel en kunnen we inspelen op actuele situaties en ontwikkelingen. Het werken in overeenstemming met de gestelde 'regels' in het IBP Normenkader is belangrijk, maar wordt tevens voorzien van een 'blik op de toekomst'. Meer dan voorheen komt de nadruk te liggen op het uitvoeren van risicoanalyses.

Om een betrouwbare en bestuurlijke rol te kunnen vervullen, werken we vanuit een strategie die is gestoeld op twee pijlers. De eerste pijler is '*risico's bewust nemen*' in plaats van '*onbewust risico lopen*'. Dat uit zich in een verschuiving van reactief naar proactief beleid. Wanneer zijn risico's nog acceptabel en beheersbaar? Het beschrijven en bepalen van de informatiebeveiligingsrisico's en maatregelen vormen hiervan een onderdeel.

De tweede pijler wordt gevormd door de ambitie om te groeien in (het niveau van) *volwassenheid*[3], zoals omschreven in *Capability Maturity Model Integration (CMMI[4]).*

[2] https://www.vohaaglanden.nl/public/Download/16/bestand/Strategisch%20plan.pdf
[3] https://www.nba.nl/siteassets/over-de-nba/ledengroepen/lio/lio-new/nba-lio-norea-handreiking-bij-volwassenheidsmodel-informatiebeveiliging-januari-2019.pdf
[4] https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration

Volwassenheidsniveau		Toelichting
1	Initieel	Initiële controls zijn niet, of slechts gedeeltelijk, gedefinieerd en/of worden op een inconsistente manier uitgevoerd en zijn sterk afhankelijk van individuen.
2	Herhaalbaar	Controls zijn aanwezig en worden op een gestructureerde en consistente, maar informele manier uitgevoerd.
3	**Gedefinieerd**	**Controls worden gedocumenteerd en op een gestructureerde en formele manier uitgevoerd. Uitvoering van controle kan worden bewezen, is getest en effectief.**
4	Beheerst en meetbaar (PDCA)	De effectiviteit van de control wordt periodiek geëvalueerd en waar nodig verbeterd. Deze beoordeling is gedocumenteerd.
5	Voortdurende verbetering	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.

Vanuit de gezamenlijke ambitie streven we ernaar om conform het op landelijk vastgesteld niveau, voor alle scholen, voor wat betreft de borging van informatiebeveiliging in 2027 op volwassenheidsniveau 3 te zitten.

Op volwassenheidsniveau 3 vinden de werkzaamheden in definieerde, gedocumenteerde en beheerste processen plaats, risico's worden ingeschat op basis van risico assessments, zijn verantwoordelijkheden en taken eenduidig toegewezen. Wordt regulier gerapporteerd omtrent de uitvoering van beheersingsmaatregel(en) aan het management. Wordt de effectieve werking van controles periodiek getoetst, gebaseerd op het risicoprofiel van de school.

Scope en doelstelling

Het normenkader waar VO Haaglanden op het gebied van Informatiebeveiliging en privacy medio 2027 aan moet voldoen is vastgelegd in het *Digitaal Funderend Onderwijs 2023 (IBP Normenkader)*[5]. Het IBP Normkader helpt proceseigenaren bij het nemen hun verantwoordelijkheid in Informatiebeveiliging. Vanuit het IBP Normenkader is een aantal eisen opgelegd waar we voor moeten zorgdragen. De norm vanuit het IBP Normenkader is dat iedere school maatregelen moet nemen om hieraan te voldoen.

De scope van het Informatiebeveiligingsbeleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van het bestuur bureau (BSB), scholen, externe partijen en het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Strategische uitgangspunten

Met betrekking tot **Informatiebeveiliging en Privacy** onderscheiden we 3 aandachtsgebieden:

1. Governance
2. Processen
3. Technische Weerbaarheid

Hiermee hebben we het volgende voor ogen:

- Iedere medewerker is verantwoordelijk voor de veiligheid van de informatie die door de organisatie beschikbaar wordt gesteld.

[5] https://sivon.nl/normenkader-ibp-fo/

- Alle leidinggevenden binnen VO Haaglanden zien erop toe dat hun medewerkers voldoende geschoold zijn en het Informatiebeveiliging en Privacy beleid naleven.
- Het College van Bestuur is eindverantwoordelijk en moet verantwoording kunnen afleggen aan, bijvoorbeeld, de Raad van Toezicht.
- Proceseigenaren zijn benoemd en zijn bewust van hun verantwoordelijkheid bij de uitvoer van processen waar Informatiebeveiliging en Privacy een belangrijke rol speelt.
- IT is verantwoordelijk voor de technische weerbaarheid.

Governance

De Governance gaat over het "wat en wie en met welk doel" en is gericht op de volgende thema's:

1. Strategie: We sluiten aan bij de organisatiestrategie.
2. Beleid: We werken binnen vastgestelde kaders.
3. Architectuur: We werken vanuit een gekozen model.
4. Eigenaarschap: We benoemen rollen en verantwoordelijkheden en delen die toe.
5. Risk Management: We prioriteren op basis van een risicoanalyse.
6. Roadmap: We leggen de te nemen acties vast in de tijd en maken daar budget voor vrij.
7. Toetsing: We laten ons toetsen.

Alle te ondernemen acties in de processen en technische weerbaarheid zijn geborgd in de Governance:
We weten wie wat doet met welk doel en in lijn met de strategische doelstellingen van de organisatie.

Het belangrijkste doel van alle maatregelen is het mitigeren van de risico's die we lopen op het gebied van Informatiebeveiliging en Privacy, waarmee we een veilige leer- en werk omgeving kunnen borgen. Certificering (goedkeuring) wordt echter een steeds belangrijker onderdeel van de Governance. Een Certificering kan alleen gegeven worden door een professionele externe auditor. Vanwege recente grote veiligheidsincidenten binnen het onderwijsveld neigt het Ministerie van Onderwijs steeds meer naar een verplichte externe audit waarbij externe verantwoording steeds belangrijker wordt.

Ter ondersteuning bij de implementatie van, toezicht op, governance, risk en compliance (GRC) zal VO Haaglanden, per februari 2024, derhalve een door het SIVON voorgestelde GRC tool in gebruik nemen. Hiermee wordt een centraal platform aangeboden om op een uniforme manier het risicomanagement proces te borgen.

IBP-processen

Bij de volgende processen speelt Informatiebeveiliging en Privacy een grote rol:

1. Human Resources: betreft borging expertise en training.
2. ITIL: betreft Incident, Problem, Change, en Configuration Management en Fysieke Beveiliging.
3. Datamanagement: betreft opslag, beheer, verwijderen (bewaartermijnen) en bescherming van gegevens.
4. Identity & Access Management (IAM): betreft toegangsregels en - rechten tot informatie.
5. Security Baselines: minimale afspraken over hoe veilig te werken
6. Business Continuity: betreft opvangen van incidenten (waaronder crisismanagement).
7. Cloud Leveranciers: goede afspraken en controle daarop bij externe leveranciers.

Aan ieder proces is een proceseigenaar toegewezen en de processen zijn beschreven en getoetst.

Technische weerbaarheid

Bij technische weerbaarheid zijn de volgende thema's te onderscheiden:

1. Multi Factor Authenticatie/Thuiswerken: betreft veilig van buitenaf inloggen.

2. SOC SIEM: betreft 24 x 7 detectie van het netwerk (en respons).
3. Pentesten: betreft periodiek gericht testen op kwetsbaarheden in het netwerk.
4. Patchbeheer: betreft structureel bijwerken van de software (beveiligingsupdates).
5. Infrastructuur: betreft beschikbaarheid van het netwerk en systemen.
6. Security Policy: betreft inrichting technische beveiliging van het netwerk en systemen.
7. Computer Operations: betreft automatische IT-processen (bijvoorbeeld back-up).

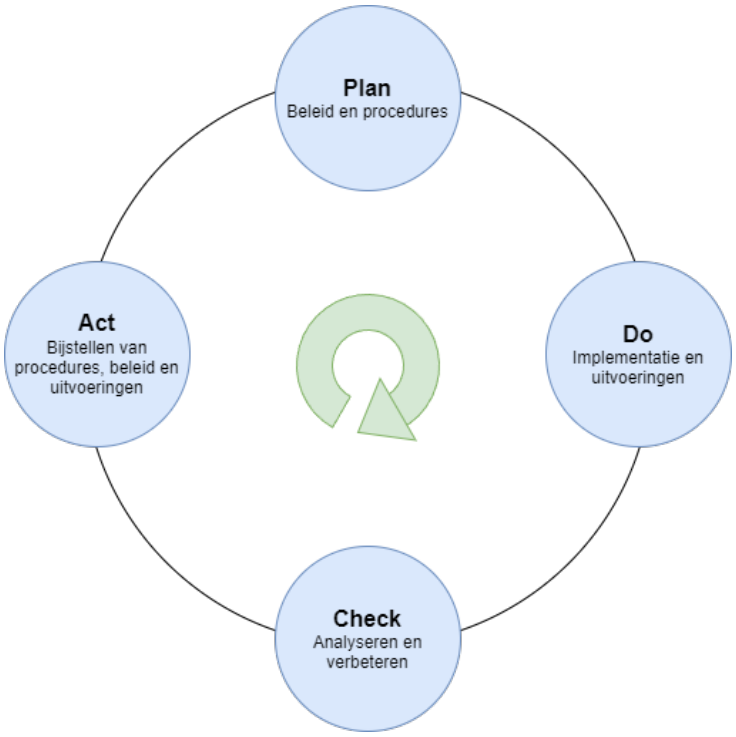
De bovenstaande thema's zullen uitgevoerd of onder regie uitbesteed worden door de IT-afdeling. Zij zullen hierover in begrijpelijke taal rapporteren aan het College van Bestuur. Bij deze rapportage hoort ook een financieel overzicht, zodat duidelijk is welke veiligheidsmaatregelen horen bij de gemaakte kosten/investeringen. Hieruit vloeit voort dat in de jaarlijkse begroting(en) rekening gehouden dient te worden met additionele uitgaven die gericht zijn op het verkleinen (of voorkomen) van informatiebeveiliging & privacy gerelateerde risico's.

De thema's Multi Factor Authenticatie/Thuiswerken, SOC SIEM en Security Policy vallen onder het zogenaamde Zero Trust principe.

Uitwerking strategisch beleid

Het strategische beleid wordt als kader en basis gebruikt voor het uitwerken van de tactische beleidsplannen. Hiermee geeft het richting voor de verdere invulling van IB binnen de operationele doelstellingen en inspanningsverplichtingen binnen VO Haaglanden. Dit zal worden vertaald in een tactisch en operationeel beleid. De werkzaamheden worden uitgewerkt in een Informatiebeveiligingsplan (IBP). Door ieder jaar een nieuw operationeel plan te schrijven, is het mogelijk om snel in te kunnen spelen op de actualiteit en andere ontwikkelingen. Het maakt VO Haaglanden flexibeler en daardoor veiliger.

Voor het gestructureerd bijhouden van de status rondom IB wordt gebruikgemaakt van de jaarlijkse PDCA-cyclus.



stichting
VO Haaglanden

Slot en vervolg

Deze visie op en strategische uitgangspunten van Informatiebeveiliging en Privacy zijn leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging en bescherming van de persoonsgegevens.

In het Informatiebeveiliging en privacy beleid zijn deze uitgangspunten uitgewerkt en gekaderd, zodat VO Haaglanden planmatig kan groeien in volwassenheid en stappen zet in de richting waar ze als organisatie voor gaat.

stichting
VO Haaglanden

Met dank aan Ludo Cuijpers, Leo Jaarsma, Henk Links, Sebastiaan van Trigt voor het basisontwerp van dit document.