

# Informatiebeveligings- en privacybeleid

2025-2029



## Versieblad

|                   |                                                    |
|-------------------|----------------------------------------------------|
| Documenttitel     | Informatiebeveiligings- en privacybeleid 2025-2029 |
| Versie            | 1.0                                                |
| Datum             | 18-03-2024                                         |
| Status            | Definitief                                         |
| Classificatie     | Openbaar                                           |
| Proceseigenaar    | A.Verwijst                                         |
| Documentbeheerder | A.Verwijst                                         |

| Wijzigingshistorie |  |  |  |
|--------------------|--|--|--|
|                    |  |  |  |
|                    |  |  |  |
|                    |  |  |  |
|                    |  |  |  |
|                    |  |  |  |

| Goedkeuring         |       |            |
|---------------------|-------|------------|
| Directievergadering | Datum | Agendapunt |
|                     |       |            |
|                     |       |            |
|                     |       |            |

# 1. Voorwoord

Het College van Bestuur van Stichting Optimus Onderwijs heeft het Informatiebeveiligings- en Privacybeleidsplan 2024-2028 vastgesteld. In een tijdperk waarin digitale transformatie onvermijdelijk en essentieel is voor het onderwijs, erkennen we het cruciale belang van adequate informatiebeveiliging en de bescherming van privacy alsmede onze verantwoordelijkheid om een veilige en vertrouwde leeromgeving te creëren. Dit beleidsplan vormt de ruggengraat van onze inspanningen om persoonsgegevens en onderwijsinformatie te beschermen tegen de toenemende dreigingen in het digitale tijdperk. Het plan is ontwikkeld in nauwe samenwerking met experts op het gebied van informatiebeveiliging en privacy, en weerspiegelt onze inzet om te voldoen aan de gestelde normen en best practices in de sector.

Informatiebeveiliging en privacybescherming integreren we zoveel als mogelijk in alle lagen van onze organisatie, van het klaslokaal tot het bestuursniveau. Dit beleidsplan dient als een levend document, dat ons zal leiden in onze besluitvorming en handelen. Het stelt ons in staat om proactief te reageren op de voortdurend veranderende technologische landschap en wettelijke vereisten.

We zijn trots op de vooruitgang die we hebben geboekt en streven naar continue verbetering. Samen met alle betrokkenen - leerlingen, ouders/verzorgers, medewerkers en partners - werken we aan een veilige toekomst waarin onderwijs en privacy hand in hand gaan.

Wij danken iedereen die heeft bijgedragen aan de ontwikkeling van dit beleidsplan en kijken uit naar de verdere implementatie ervan in de komende jaren.

Met vriendelijke groet,

Drs. M.A.M. (Monique) Donders RA Voorzitter College van Bestuur Stichting Optimus Onderwijs

## 2. Informatiebeveiliging- en privacyreglement

### 2.1 Het belang van informatiebeveiliging en privacy

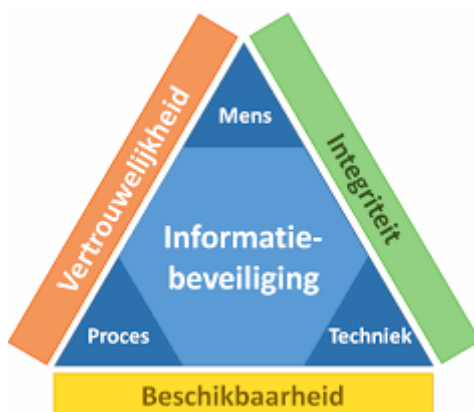
Het onderwijs vertrouwt steeds meer op informatie en ICT. De hoeveelheid informatie, inclusief persoonlijke gegevens, groeit vanwege ontwikkelingen op het gebied van ICT binnen en buiten de onderwijsorganisatie. Het is van groot belang om informatie adequaat te beschermen en verantwoordelijk om te gaan met persoonlijke gegevens. De continue ontwikkeling op het gebied van ICT en de benodigde bescherming van persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het opstellen van een solide beleid voor informatiebeveiliging en privacy (afgekort als IBP) is essentieel om de gevolgen van deze risico's te minimaliseren tot een aanvaardbaar niveau en tegelijkertijd de voortgang van het onderwijs en de efficiëntie van de bedrijfsvoering te waarborgen.

### 2.2 Toelichting informatiebeveiliging

Informatiebeveiliging betekent dat we verschillende stappen nemen en regels volgen om ervoor te zorgen dat informatie altijd betrouwbaar blijft. We willen dat informatie altijd beschikbaar is wanneer we die nodig hebben (beschikbaarheid), dat het klopt en compleet is (integriteit), en dat alleen de mensen die toestemming hebben, toegang krijgen tot die informatie (vertrouwelijkheid). Het is belangrijk om te begrijpen hoe we informatie veilig kunnen houden. Daarnaast is het integreren van veerkracht in onze beveiligingsstrategieën essentieel.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot verstoring van het onderwijsproces en mogelijk (financiële) schades en imagooverlies.

In aanvulling op de reeds genoemde aspecten van informatiebeveiliging, willen we de volgende kerncomponenten benadrukken:



- **Beschikbaarheid:** We streven ernaar dat gegevens en functionaliteit zodanig beschikbaar zijn voor onze medewerkers dat zij hun taken optimaal kunnen uitvoeren. Dit betekent dat essentiële informatie en systemen toegankelijk moeten zijn wanneer nodig, om de continuïteit van het onderwijsproces te waarborgen. Hierbij rekening houdend met de bewaar- en vernietigingsverplichting.

- **Integriteit:** De juistheid en actualiteit van onze gegevens en systemen is cruciaal. Dit vereist dat deze gegevens en functionaliteit te allen tijde voldoen aan de daarvoor gestelde normen en wet- en regelgeving, om te garanderen dat onze besluitvorming en onderwijsprocessen gebaseerd zijn op betrouwbare informatie.
- **Vertrouwelijkheid:** Het beschermen van informatie tegen ongeautoriseerde kennisname en wijziging is een prioriteit. Dit betekent dat de toegang tot (persoons)gegevens en systemen strikt beperkt is tot personen die daartoe expliciet door Stichting Optimus Onderwijs zijn aangewezen.
- **Controleerbaarheid:** Het is van belang dat verwerkingen, handelingen en besluiten binnen onze organisatie in relatie tot IBP aantoonbaar en controleerbaar zijn. Dit draagt bij aan de transparantie en het vertrouwen in onze processen en zorgt ervoor dat we kunnen verifiëren dat de getroffen beveiligingsmaatregelen effectief zijn en naar behoren functioneren.

Deze elementen vormen de basis van ons streven naar een veilige en betrouwbare informatieomgeving, wat essentieel is voor het handhaven van de kwaliteit en integriteit van ons onderwijs.

## 2.3 Toelichting privacy

Privacy draait om het beschermen van persoonsgegevens, wat volgens de huidige wetten en regels moet gebeuren. Het regelt onder welke voorwaarden we persoonlijke gegevens mogen gebruiken. Persoonsgegevens zijn alle gegevens die direct of indirect kunnen laten zien wie een persoon is.

Het verwerken van persoonsgegevens omvat allerlei handelingen, zoals het verzamelen, opslaan, aanpassen, bekijken, gebruiken, delen en zelfs het verwijderen van deze gegevens. Dit is wettelijk vastgelegd en omvat verschillende acties, van het verzamelen van gegevens tot het vernietigen ervan.

Kort gezegd, privacy gaat over het zorgvuldig omgaan met persoonlijke informatie volgens de wet, om ervoor te zorgen dat iemands gegevens veilig blijven.

### De samenhang tussen Informatiebeveiliging en Privacy

Zoals we eerder hebben besproken, is informatiebeveiliging cruciaal om de privacy te waarborgen. Omgekeerd geldt dat het zorgvuldig omgaan met persoonsgegevens essentieel is voor goede informatiebeveiliging.

Informatiebeveiliging en privacy zijn sterk met elkaar verweven. Daarom worden ze samengevoegd tot één proces, wat we het IBP-proces noemen. Dit proces, dat verder wordt aangeduid als het IBP-beleid, vormt het fundament waarop we de beveiliging van informatie en privacy binnen Stichting Optimus Onderwijs baseren. Het fungeert als leidraad voor de regels en procedures die hieronder vallen.

## 3. Over dit beleidsdocument

### 3.1 Doel, toepassingsgebied en gebruikers

We dragen zorg voor drie belangrijke doelen:

- Zorgen dat het onderwijs en de schooladministratie altijd goed blijven werken.
- Ervoor zorgen dat de persoonsgegevens van iedereen die bij Stichting Optimus betrokken is - zoals leerlingen, ouders/verzorgers en medewerkers - altijd wordt gerespecteerd en beschermd.
- Voorkomen dat er beveiligings- en privacyproblemen optreden, en als ze toch gebeuren, de gevolgen hiervan beperken.

Het IBP-beleid is ontworpen om de manier waarop we informatie verwerken en persoonsgegevens beveiligen te borgen of te verbeteren. Hierbij streven we naar een juiste balans tussen privacy, functionaliteit en veiligheid. Het belangrijkste uitgangspunt is het respecteren van de persoonlijke levenssfeer van betrokkenen, zoals medewerkers, leerlingen en hun ouder(s)/verzorger(s).

Dit beleid zorgt ervoor dat Stichting Optimus Onderwijs voldoet aan alle relevante wet- en regelgeving, terwijl we tegelijkertijd zorgen voor de bescherming van persoonlijke gegevens en een efficiënte werking van onze systemen.

Ons IBP-beleid bij Stichting Optimus Onderwijs geldt voor iedereen, zoals medewerkers, leerlingen, ouders/verzorgers, bezoekers, vrijwilligers, en externe partners. Het geldt ook voor alle apparaten die toegang geven tot ons netwerk.

- Dit beleid is gericht op het definiëren van het doel, de richting, de principes en de basisregels voor Informatiebeveiliging.
- Dit beleid omvat het verwerken van persoonsgegevens van alle schoolgemeenschapsleden, inclusief medewerkers, leerlingen, ouders/verzorgers, bezoekers en externe partners, voor alle toepassingen onder onze verantwoordelijkheid, inclusief externe informatie op websites en sociale media.
- Dit beleid is van toepassing op alle geautomatiseerde en handmatige verwerking van persoonsgegevens die onder onze verantwoordelijkheid vallen, inclusief de bijbehorende documenten die in onze bestanden zijn opgenomen. Dit betekent dat we zorgvuldig omgaan met alle informatie over mensen, zowel digitaal als op papier.
- Wanneer de doeltreffendheid van dit document wordt beoordeeld, dan dient het aantal incidenten in verband met het niet volgen van dit beleid, en het aantal incidenten in verband met het ontbreken van beleid, in ogenschouw te worden genomen.
- Dit beleid vertoont raakvlakken met diverse beleidsdocumenten van Stichting Optimus Primair Onderwijs, namelijk:
  - Schoolveiligheidsplan
  - Logisch toegangsbeveiligingsbeleid
  - Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
  - ICT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen.
  - ICT- gedragscode bedrijfsmiddelen

## 3.2 Gerefereerde documenten

In het kader van informatiebeveiliging en privacy heeft de organisatie verwezen naar de volgende relevante documenten en normen:

- Normenkader Informatie en Veiligheid
- ISO/IEC 27001 norm, clause 5.2
- ISMS-document
- Technisch Beleid

## 3.3 Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming
- Uitvoeringswet AVG
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

## 3.4 Geldigheid en documentbeheer

Dit document is geldig vanaf de definitieve versie datum.

Door Optimus Primair Onderwijs wordt het IBP-beleidsplan iedere vier jaar herzien. Het College van Bestuur is eindverantwoordelijk voor het beleid.

## 3.5 Goedkeuring van dit het beleid

Hierbij bevestigt het College van Bestuur de geldigheid van dit beleid.

Drs. M.A.M. (Monique) Donders RA

Voorzitter College van Bestuur Stichting Optimus Onderwijs

## 4. Uitgangspunten IBP-beleid

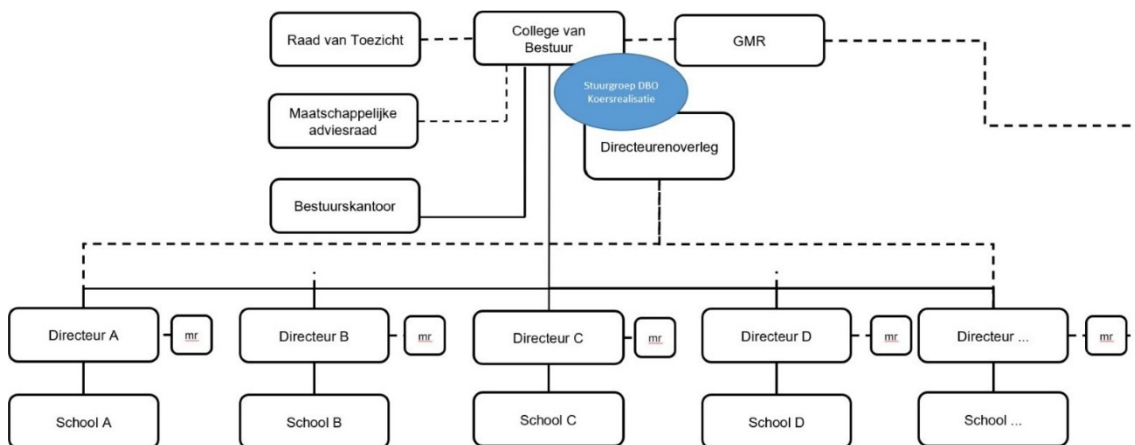
Stichting Optimus Onderwijs hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

- Het College van Bestuur is eindverantwoordelijk voor informatiebeveiliging en privacy.
- Het College van Bestuur moet ervoor zorgen dat voldaan wordt aan wet- en regelgeving en stellen het kader vast waaraan alle scholen en alle medewerkers zich dienen te houden.
- Als we persoonsgegevens gebruiken, moeten we altijd een goede reden hebben en de wet volgen. We respecteren de privacy van mensen.
- We vertellen iedereen duidelijk hoe we hun gegevens gebruiken en wat hun rechten zijn.
- We houden een register bij van gegevens die we gebruiken en houden dit actueel.
- Iedereen moet zorgen voor veiligheid, zowel digitaal als met papieren documenten.
- We zijn eigenaar van onze informatie en respecteren ook de informatie van anderen.
- We bekijken welke risico's er zijn en wat we moeten doen om ze te verminderen.
- We maken afspraken met bedrijven die gegevens voor ons verwerken.
- We verwachten goed gedrag van iedereen en hebben regels hiervoor.
- We controleren en passen onze aanpak elk jaar aan.
- Voordat we iets veranderen in onze systemen, kijken we naar de invloed op beveiliging en privacy en nemen we maatregelen.
- We gebruiken technologie om gegevens te beschermen.
- We houden bij als er beveiligingsproblemen zijn en melden die aan de juiste instanties.
- We hanteren het principe van 'Alles is in principe verboden, tenzij het uitdrukkelijk is toegestaan' met betrekking tot informatiebeveiliging (autorisatie en authenticatie). Deze benadering is strenger dan de alternatieve regel 'Alles is in principe toegestaan, tenzij het uitdrukkelijk is verboden.' Dit benadrukt ons striktere beleid en de noodzaak van expliciete toestemming voor toegang tot informatie en systemen
- De Privacy en Security Officer ervoor te zorgen dat alle medewerkers van Optimus die betrokken zijn, alsmede relevante externe partijen bekend zijn met dit beleid.

## 5. Organisatie

### 5.1 Optimus organisatie

Organogram Stichting Optimus Primair Onderwijs.



In onze stichting staan de leerling en de leerkracht centraal. Directeur, ib'er en ondersteunend personeel zorgen dat de leerkracht zijn werk zo goed mogelijk kan doen. Achter de scholen staat het bestuur, de staf en diverse organen om alle processen die het primaire proces dienen optimaal in te richten, uit te voeren en te controleren.

#### College van bestuur

Het College van Bestuur is verantwoordelijk voor de kwaliteit, strategie, communicatie en belangenbehartiging bij Optimus. Ze leggen verantwoording af aan de samenleving.

#### Raad van Toezicht

De Raad van Toezicht vertegenwoordigt de samenleving, houdt toezicht op de organisatie en is werkgever en klankbord voor het College van Bestuur. Voor belangrijke besluiten van het College van Bestuur is goedkeuring van de Raad van Toezicht vereist. De Raad van Toezicht bestaat uit meerdere leden.

#### Directeur

Directeuren functioneren als integraal schoolleiders. Ze hebben regelmatig beleidsoverleg (DBO) met elkaar en met de bestuurders. Iedere directeur heeft één van de bestuurders als eerste aanspreekpunt. De directeur legt verantwoording aan de bestuurders af.

#### Bestuurskantoor

Het bestuurskantoor ondersteunt de bestuurders en schooldirecteuren. Het bestuurskantoor bestaat uit de domeinen: Onderwijs, Innovatie & Kwaliteit, HRM, Bestuurssecretariaat en Bedrijfsvoering. Een volledig overzicht is te vinden op onze [website](https://optimusonderwijs.nl/over-optimus/organisatie/bestuurskantoor).  
[optimusonderwijs.nl/over-optimus/organisatie/bestuurskantoor](https://optimusonderwijs.nl/over-optimus/organisatie/bestuurskantoor)

#### Scholen

Onze stichting omvat veertig scholen, waaronder twee SBO-scholen, gelegen in de provincie Noord-Brabant. Zie Bijlage 1 | Locaties scholen Stichting Optimus Primair Onderwijs voor een locatieoverzicht van onze scholen.

## 6. Governance – Rol, betrokkenheid en verantwoordelijkheid

### 6.1 Regie-organisatie

Binnen Stichting Optimus Onderwijs hanteren we de aanpak van een regie-organisatie. Dit betekent dat het bestuur, directeuren en de staf de leiding nemen in het vaststellen van de koers en de strategische planning. De uitvoering van deze strategieën vindt plaats op de scholen zelf.

Centraal in onze aanpak staat dat we de autonomie en de eigenheid van elke school binnen de stichting erkennen en respecteren. Tegelijkertijd zorgen we ervoor dat de overkoepelende doelen en beleidslijnen van de stichting consequent worden nageleefd en uitgevoerd.

Het College van Bestuur speelt hierin een cruciale rol. Zij zijn verantwoordelijk voor het vaststellen van de kwaliteitsnormen, het formuleren van de strategische doelen en het voeren van de algehele regie. Dit gebeurt in nauwe samenwerking met de Raad van Toezicht, die de belangen van de samenleving vertegenwoordigt en toezicht houdt op de naleving van deze doelen en normen.

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken hebben we voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

### 6.2 Richtinggevend - Eindverantwoordelijke

Het College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.

De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd. De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de Privacy en Security Officer.

| Niveau                              | Wie Rollen          | Verantwoordelijk voor:                                                                                                                                                                                                                                                                                                                                    | Wat: (Realiseren/ vastleggen)                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Eindverantwoordelijke (strategisch) | College van Bestuur | <ul style="list-style-type: none"><li>• IBP-beleidsvorming, vastlegging en het uitdragen ervan</li><li>• Voor het verzekeren dat alle fasen in de implementatie van het ISMS<sup>1</sup> en de voortdurende verbetering worden ondersteund met passende middelen om zowel de doelen en doelstellingen van dit beleid te bereiken als te voldoen</li></ul> | <ul style="list-style-type: none"><li>• Informatiebeveiligings- en privacybeleid vaststellen</li><li>• Draagt zorg dat iedereen die betrokken is bij het ISMS, bekend is met dit beleid.</li><li>• Regelmatig de naleving van informatieverwerkingsprocedures controleren volgens de geldende beleidsregels, normen en beveiligingseisen.</li></ul> |

|  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p>aan alle geïdentificeerde vereisten</p> <ul style="list-style-type: none"> <li>• Voor de naleving van het geldende informatiebeveiligingsbeleid, normen en andere beveiligingseisen binnen hun verantwoordelijkheidsgebied</li> <li>• Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens</li> <li>• Evalueren toepassing en werking IBP-beleid op basis van rapportages</li> <li>• Strategische aspecten normenkader invulling geven.</li> </ul> | <ul style="list-style-type: none"> <li>• Het College van Bestuur verlangt dat domeinbeheerders regelmatig beoordelen of de informatieverwerking voldoet</li> <li>• Verlangt van de domeinbeheerders dat indien als resultaat van de beoordeling een geval van niet- naleving wordt ontdekt dat: <ul style="list-style-type: none"> <li>a. de oorzaken van deze niet-naleving vaststellen;</li> <li>b. de noodzaak voor handelen beoordelen om te waarborgen dat niet-naleving zich niet opnieuw voordoet;</li> <li>c. passende corrigerende maatregelen vaststellen en implementeren;</li> <li>d. de uitgevoerde correctieve maatregel beoordelen</li> </ul> </li> <li>• Reglementen vaststellen</li> <li>• Communicatie naar Directeurenoverleg/ RvT</li> <li>• Voor de naleving van het geldende informatiebeveiligingsbeleid, normen en andere beveiligingseisen binnen hun verantwoordelijkheidsgebied, verlangt het College van Bestuur dat domeinbeheerders<sup>2</sup> regelmatig beoordelen of de informatie-verwerking voldoet.</li> </ul> |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

<sup>1</sup> Managementsysteem voor informatiebeveiliging

<sup>2</sup> Afdelingshoofden, schooldirecteuren, proceseigenaren

## 6.3 Privacy en Security Officer

Privacy en Security Officer is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau. De rol van de Privacy en Security Officer is:

| Niveau  | Wie Rollen                  | Verantwoordelijk voor:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Wat: (Realiseren/ vastleggen)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sturend | Privacy en Security Officer | <ul style="list-style-type: none"><li>• Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling;</li><li>• De toepassing en naleving van het informatiebeveiligings- en privacybeleid monitoren;</li><li>• De uniformiteit bewaken binnen Stichting Optimus Onderwijs;</li><li>• Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy;</li><li>• De verdere afhandeling van incidenten binnen Stichting Optimus Primair Onderwijs coördineren</li><li>• IBP-planning en controle Adviseert bestuur/College van Bestuur /directie over IBP Voorbereiden uitvoeren IBP- beleid, Classificatie/risicoanalyse Hanteren IBP-normen en wijze van toetsen;</li><li>• Sturing, advisering en controleren bieden in het "AVG- PDCA op school" programma.</li></ul> | Processen, richtlijnen en procedures IBP, waaronder: <ul style="list-style-type: none"><li>• Voortgang gegeven aan de gesprekkencyclus als onderdeel van het AVG- PDCA op school" programma.</li><li>• Autorisatiebeheer en controle</li><li>• Logboekcontrole</li><li>• Beveiligingsincidenten en datalekken</li><li>• Verwerkersovereenkomsten toetsen en advies uitbrengen</li><li>• Bewustzijn medewerkers (stichtingbreed) vergroten middels AVG website, posters, voorlichting op scholen, enz.</li><li>• Hulp en vraagbaak zijn voor medewerkers, in het bijzonder voor staf en domeinverantwoordelijken.</li></ul> |

## 6.4 Functionaris voor Gegevensbescherming

Onze Functionaris voor Gegevensbescherming (FG) houdt toezicht op hoe we de AVG naleven bij Stichting Optimus Primair Onderwijs. De FG heeft wettelijke taken en bevoegdheden waardoor hij onafhankelijk in onze organisatie opereert. Hij werkt aan het vergroten van bewustzijn over Informatiebeveiliging en Privacy (IBP), behandelt incidenten met betrekking tot informatiebeveiliging, geeft advies over privacyzaken, onderhoudt eventuele contacten met de Autoriteit Persoonsgegevens (AP), en rapporteert aan het bestuur, onze hoogste verantwoordelijke. De FG heeft regelmatig overleg met onze Privacy en Security Officer en fungeert als aanspreekpunt voor klachten en vragen van betrokkenen.

| Niveau             | Wie Rollen                       | Verantwoordelijk voor:                                                                                                                                                                                                                                                                                                                       | Wat: (Realiseren/ vastleggen)                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sturend (tactisch) | Functionaris gegevensbescherming | <ul style="list-style-type: none"> <li>• Toezicht op naleving privacywetgeving</li> <li>• Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens</li> <li>• Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door College van Bestuur.</li> </ul> | <ul style="list-style-type: none"> <li>• Steekproefcontrole scholen</li> <li>• Privacyreglement, procedure IBP-incident afhandeling</li> <li>• Afwikkeling klachten en incidenten</li> <li>• Advisering Privacy en Security Officer</li> <li>• Onderhoudt contacten met Autoriteit Persoonsgegevens</li> <li>• Rapporteert aan het College van Bestuur</li> <li>• Classificatie/risicoanalyse in samenwerking met Privacy en Security Officer</li> </ul> |

## 6.5 Externe accountant/ externe auditor

De externe accountant speelt een cruciale rol in het waarborgen van de financiële integriteit en transparantie van organisaties. Als onafhankelijke en objectieve expert voert de accountant audits uit op jaarrekeningen, beoordeelt de naleving van wettelijke voorschriften en bedrijfsprocessen, en biedt vertrouwen aan belanghebbenden over de betrouwbaarheid van de financiële verslaggeving. De externe accountant is niet alleen een controleur van feiten, maar ook een waardevolle adviseur die inzichten biedt voor het verbeteren van de bedrijfsvoering, het risicobeheer en de efficiëntie. Binnen het domein van Informatiebeveiligingsplan (IBP) omvat de rol van de externe accountant/auditor:

| Niveau             | Wie Rollen                          | Verantwoordelijk voor:                                                                                                                                                                                                                                                                                                                                                                                                                             | Wat: (Realiseren/ vastleggen)                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sturend (tactisch) | Externe accountant/ externe auditor | <ul style="list-style-type: none"> <li>• Naleving Wet- en Regelgeving: Zekerheid bieden over de naleving van relevante wet- en regelgeving, met implicaties voor informatiebeveiliging en privacywetgeving.</li> <li>• Advisering over Administratieve Organisatie en Interne Beheersing: Advies geven op het gebied van administratieve organisatie en interne beheersing, wat fundamenteel is voor informatiebeveiligingsmaatregelen.</li> </ul> | <ul style="list-style-type: none"> <li>• Controle van Processen: Uitvoeren van een interimcontrole gericht op processen zoals inkoop, betaling en automatisering. Deze controle is relevant voor het identificeren van risico's en controlepunten voor het IBP.</li> <li>• Automatisering en IT Audit: Aandacht besteden aan automatisering en IT-audits, die cruciale inzichten kunnen bieden voor het IBP, vooral met betrekking tot de beveiliging van informatiesystemen en data.</li> </ul> |

## 6.6 Domeinverantwoordelijke en of stafmedewerkers

Bij Stichting Optimus Primair Onderwijs hebben we de volgende domeinen: Onderwijs, Innovatie & Kwaliteit, HRM, Bestuurssecretariaat en Bedrijfsvoering. De eigenaren van deze domeinen en/of stafmedewerkers dragen de verantwoordelijkheid voor het opvolgen van de richtlijnen, procedures en instructies. Ze zijn ook belast met het signaleren van risico's die kunnen ontstaan wanneer personen of applicaties ongeautoriseerde toegang krijgen tot onze systemen.

| Niveau             | Wie Rollen                                    | Verantwoordelijk voor:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Wat: (Realiseren/vastleggen)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sturend (tactisch) | Domeinverantwoordelijke en of stafmedewerkers | <ul style="list-style-type: none"> <li>• Cultiveren van een sterke AVG- "gegevensveiligheidscultuur" binnen het domein.</li> <li>• Samenwerken met Privacy en Security Officer om geautoriseerde toegang op basis van functie en taak tot netwerken en diensten te waarborgen.</li> <li>• Voorafgaand aan de aanschaf van nieuwe software-systemen, advies aanvragen bij de Privacy en Security Officer</li> <li>• Op aanvraag van de Privacy en Security Officer beveiligingsgegevens aanleveren.</li> <li>• Direct rapporteren van vermoedelijke beveiligingsincidenten en datalekken aan ICT-beheer en de Privacy en Security Officer</li> <li>• Bij verzoeken van externe instanties om persoonsgegevens te verstrekken, tijdig de Privacy en Security Officer informeren en advies vragen over de te nemen stappen.</li> </ul> | <ul style="list-style-type: none"> <li>• Zorgvuldig beheren van persoonlijke inloggegevens.</li> <li>• Het veilig gebruik van apparatuur conform de richtlijnen in de ICT-gedragscodes voor bedrijfsmiddelen naleven.</li> <li>• Indien gevraagd, samenwerken met de Privacy en Security Officer om autorisatiegegevens te verstrekken voor controles van hoog-risicosystemen.</li> <li>• Opvolgen van aanbevelingen van de Privacy en Security Officer met betrekking tot onmiddellijke beveiligingskwesaties en passende maatregelen treffen.</li> </ul> |

## 6.7 Schooldirecteur/ leidinggevende

De directeuren hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

| Niveau                     | Wie Rollen                         | Verantwoordelijk voor:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Wat: (Realiseren/ vastleggen)                                                                                                                                                                                                                                                                                                      |
|----------------------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Uitvoerend<br>Operationeel | Schooldirecteur/<br>leidinggevende | <ul style="list-style-type: none"><li>• Implementeren van AVG-beheersmaatregelen uit het "AVG- PDCA op school" programma.</li><li>• Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid.</li><li>• Samen met Privacy en Security Officer zorgen voor alleen geautoriseerde toegang op basis van functie en taak tot netwerk en diensten.</li><li>• Controleren software op beveiligingseisen bij Privacy en Security Officer voor inkoop en gebruik.</li><li>• Samen met ICT-beheer en de Privacy en Security Officer zorgdragen voor de beveiliging van apparaten met antivirus en firewalls, vooral voor schoolsoftware.</li><li>• Voorafgaand aan de aanschaf van nieuwe softwaresystemen, advies aanvraag indienen bij de Privacy en Security Officer.</li><li>• Op aanvraag van de Privacy en Security Officer beveiligingsgegevens aanleveren.</li><li>• Onmiddellijk melden van vermoede beveiligings- en datalekken aan ICT- beheer en de Privacy en Security Officer.</li></ul> | <ul style="list-style-type: none"><li>• Deelnemen aan AVG-PDCA gesprekscyclus.</li><li>• Uitvoering geven aan de AVG-beheersmaatregelen.</li><li>• Bewust omgaan met Privacy en Security Officer en hier een voorbeeldfunctie vervullen.</li><li>• Bewustzijnsmateriaal geleverd vanuit AVG binnen het team overbrengen.</li></ul> |

## 6.8 Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in het personeelshandboek Stichting Optimus Onderwijs. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met infographics, checklists en formulieren.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR).

## 7. Compliance – Wat we doen

We geven hier een praktische invulling van bovenstaande beleidspunten en daarmee de minimale invulling van het beleid.

### 7.1 Informatiebeveiliging binnen Optimus

#### 7.1.1 Normenkader informatiebeveiliging

We volgen de richtlijn Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs (IBP FO), inclusief de bijbehorende normen. Elk van deze normen heeft bijbehorende evaluatiecriteria (toetsingskaders) die het minimale niveau beschrijven waarnaar onze sector streeft. Stichting Optimus heeft als doel om tegen medio september 2027 ten minste te voldoen aan deze minimale normen. De evaluatie zal worden uitgevoerd aan de hand van de eerdergenoemde toetsingskaders.

#### 7.1.2 Basisterminologie Informatiebeveiliging

- **AVG** – Algemene Verordening Gegevensbescherming.
- **Bedrijfsmiddelen** - in de context van dit beleid wordt de term bedrijfsmiddelen toegepast op informatie systemen en andere informatie-apparatuur, inclusief papieren documenten, mobiele telefoons, draagbare computers, media voor gegevensopslag, enz.
- **Beschikbaarheid** – kenmerk van de informatie dat de informatie beschikbaar is voor bevoegde personen als de informatie nodig is.
- **Datalek** – inbreuk in verband met persoonsgegevens - een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (artikel 4, lid 12 AVG).
- **Informatiebeveiliging** - behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.
- **Informatiesystemen** - Bevatten alle servers en clients, netwerkinfrastructuur, systeem en ondersteuning bij programmeren, gegevens en andere computer subsystemen en onderdelen die eigendom zijn van of worden gebruikt door de organisatie of die onder de verantwoordelijkheid van de organisatie vallen. Het gebruik van informatiesystemen bevat alle interne en externe diensten, zoals internettoegang, e-mail, enz.
- **Integriteit** – kenmerk van de informatie dat de informatie alleen op voorgeschreven wijze kan worden gewijzigd door bevoegde personen of systemen.
- **Managementsysteem voor Informatiebeveiliging (ISMS)** – deel van het gehele managementproces dat zorgdraagt voor de planning, implementatie, het onderhoud, de beoordeling, en het verbeteren van de informatiebeveiliging.
- **Persoonsgegevens** - alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online indicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4, lid 1 AVG).
- **Pseudonimisering** - het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze

aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld (artikel 4, lid 5 AVG).

- **Vertrouwelijkheid** - kenmerk van de informatie dat deze alleen beschikbaar is voor bevoegde personen of systemen.
- **Verwerker** - een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (artikel 4, lid 8 AVG).
- **Verwerkingsverantwoordelijke** – een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4, lid 7 AVG).

### 7.1.3 Eigendom van informatie

Alle gegevens die worden gecreëerd, opgeslagen, verzonden of ontvangen via informatiesystemen van Stichting Optimus Primair Onderwijs, inclusief verscheidene applicaties, e-mail, internet, enz., of het persoonlijk is of niet, moeten worden beschouwd als eigendom van de organisatie.

### 7.1.4 Risicoanalyse, Classificatie, labeling en behandeling van informatie

We waarderen alle informatie, dus we classificeren en labelen gegevens, systemen en informatie op basis van hun belang. De beveiligingsmaatregelen die we nemen, variëren afhankelijk van deze classificatie. We bepalen deze classificatie op basis van risicoanalyses, waarbij we leten op beschikbaarheid, integriteit en vertrouwelijkheid. We hebben een Beleid voor Classificatie, labeling en behandeling van informatie.

Bij veranderingen in onze systemen onderzoeken we zorgvuldig hoe dit de beveiliging en privacy beïnvloedt. De Privacy en Security Officer wordt hierbij betrokken en geeft advies. Software voor gebruik binnen de scholen wordt na classificatie op en zogeheten 'groene lijst' voor goedgekeurde- en een 'rode lijst' voor afgekeurde toepassingen geplaatst, deze is openbaar beschikbaar en te vinden via onze AVG- website ([www.Optimus.nl/AVG](http://www.Optimus.nl/AVG))

### 7.1.5 Beheer en bewaking van autorisaties en logboekregistratie

We controleren regelmatig de autorisaties van systemen met een hoog risico, minstens één keer per kwartaal. Dit wordt gecoördineerd door de Privacy en Security Officer. Daarnaast houden we logs bij van gebeurtenissen op hoog risicosystemen, zoals inlog- en uitlogacties. De Privacy en Security Officer is verantwoordelijk voor het toezicht op deze activiteiten en kan verzoeken indienen voor logboekcontroles indien nodig. Afwijkingen worden opgevolgd middels de procedure informatiebeveiligingsincidenten.

### 7.1.6 Rapportage Informatiebeveiligingsincidenten

Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.

- a. Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.
- b. Alle beveiligingsincidenten worden gemeld aan de Privacy en Security Officer. De Privacy Security Officer legt (indien nodig) de melding vast in het incidentenregister.
- c. Vermissing of diefstal van apparatuur of media die gegevens bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.
- d. Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken.

### **7.1.7 Rapportage zwakke plekken**

Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie eisen wij dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging rapporteren.

Elke werknemer, leverancier of derde partij die in contact komt met data en/of systemen van de organisatie dient elke zwakke plek, incident of gebeurtenis te rapporteren als een (mogelijk) incident, zoals gespecificeerd in de Procedure voor Incidentbeheer.

## **7.2 Privacy binnen Optimus**

### **7.2.1 Normenkader Privacy**

Om te voldoen aan de AVG-wetgeving nemen we de benodigde maatregelen. We hebben duidelijk AVG-beleid, reglementen en protocollen opgesteld, die je kunt raadplegen op de website OptimusAVG.nl. Daarnaast vind je wettelijk verplichte documenten openbaar beschikbaar op onze website. Elk jaar stelt de Privacy en Security Officer een AVG-actie/jaarplan op, dat pas wordt uitgevoerd nadat het College van Bestuur ermee heeft ingestemd. We evalueren dit actie/jaarplan in samenwerking met het College van Bestuur en de Functionaris voor Gegevensbescherming (FG).

### **7.2.2 Basisregels bij het omgaan met persoonsgegevens**

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de vijf vuistregels met betrekking tot de omgang met persoonsgegevens te weten: =

1. Doelbepaling en doelbinding: We mogen persoonsgegevens alleen gebruiken voor specifieke en rechtmatige doeleinden. Deze doelen moeten duidelijk en van tevoren worden vastgesteld. Persoonsgegevens mogen niet voor andere doeleinden worden verwerkt dan waarvoor ze zijn verzameld.
2. Grondslag: We mogen persoonsgegevens alleen verwerken als we een geldige wettelijke basis hebben om dat te doen. Er zijn zes wettelijke grondslagen die we moeten volgen
3. Dataminimalisatie: We moeten de hoeveelheid en het soort persoonsgegevens beperken tot wat redelijkerwijs nodig is om het beoogde doel te bereiken. Dit betekent dat we alleen de gegevens verzamelen die echt nodig zijn en dat we deze gegevens niet langer bewaren dan nodig is.
4. Transparantie: We moeten duidelijk en begrijpelijk aan betrokkenen (zoals leerlingen, ouders/verzorgers en medewerkers) uitleggen hoe we hun persoonsgegevens gebruiken en wat ons beleid is op het gebied van informatiebeveiliging en privacy. Deze informatie moet actief worden verstrekt. Betrokkenen hebben ook rechten, zoals het recht op correctie, verwijdering of afscherming van hun gegevens, evenals het recht om zich te verzetten tegen het gebruik van hun gegevens.
5. Data-integriteit: We moeten maatregelen nemen om ervoor te zorgen dat de persoonsgegevens die we verwerken juist en actueel zijn.

### **7.2.3 OptimusAVG.nl, een centrale hub**

De OptimusAVG-website fungeert als een toegankelijk platform dat tot doel heeft informatie, richting en ondersteuning te bieden met betrekking tot de AVG. Het biedt waardevolle hulp aan de medewerkers van de stichting en fungeert als een centrale hub en startpunt voor alle AVG-gerelateerde zaken.

#### **7.2.4 Pro-actief werken aan bewust handelen**

Bij het beheersen van risico's op het gebied van informatiebeveiliging en privacy is beleid en het nemen van maatregelen niet voldoende. Menselijke factoren spelen hierbij een cruciale rol. Daarom streven we er voortdurend naar om het bewustzijn van onze medewerkers te vergroten, zodat ze zich meer bewust worden van de risico's en veilig en verantwoord gedrag aanmoedigen. Onderdeel van ons beleid om dit te bereiken, omvat onder andere AVG-presentaties voor schoolteams, PDCA-gesprekken met betrekking tot AVG, het delen van AVG-informatie via posters en de OptimusAVG-website. Het verhogen van het bewustzijn over informatiebeveiliging en privacy is een gezamenlijke inspanning, waarbij de Privacy en Security Officer, de Functionaris Gegevensbescherming (FG), en de schooldirecteuren betrokken zijn, met het bestuur als uiteindelijk verantwoordelijke partij. Elke medewerker ontvangt bij indiensttreding een privacyreglement en de ICT-gedragscode voor bedrijfsmiddelen.

#### **7.2.5 PDCA AVG binnen de scholen**

Binnen onze stichting hebben we praktische en haalbare AVG-beheersmaatregelen ontwikkeld voor al onze scholen, die we hebben onderverdeeld in de volgende vier thema's:

- Beveiliging van persoonsgegevens
- Rechten van betrokkenen
- Bewustwording
- Bewaar- en vernietigingsverplichtingen

Om ervoor te zorgen dat deze maatregelen effectief worden toegepast, houden we twee keer per jaar gesprekken tussen de Privacy en Security Officer en de verantwoordelijke directeuren. Tijdens deze gesprekken bespreken we alle beheersmaatregelen en, indien nodig, maken we verbeterafspraken die we vastleggen in de Microsoft Planner. Onze PDCA-cyclus heeft een looptijd van vier jaar, en we streven ernaar dat alle scholen tegen 2027 voldoen aan de gestelde beheersmaatregelen binnen de vier thema's. De dagelijkse leiding en de schooldirecteuren dragen de verantwoordelijkheid voor de uitvoering van deze afspraken en het blijvend voldoen aan de AVG-beheersmaatregelen.

De Privacy en Security Officer houdt toezicht op de ontwikkeling, implementatie en naleving van deze AVG-beheersmaatregelen binnen Optimus. Bovendien rapporteert de Privacy en Security Officer regelmatig over de voortgang van deze maatregelen aan het College van Bestuur

Gedetailleerde informatie over de implementatie van deze thema's en de bijbehorende beheersmaatregelen is verder te vinden op [OptimusAVG.nl/beheersing](https://OptimusAVG.nl/beheersing)

#### **7.2.6 Data Protection Impact Assessment (DPIA)**

Voor bepaalde gegevensverwerkingen met een hoog risico is het verplicht om een Data Protection Impact Assessment (DPIA) uit te voeren. Stichting Optimus Onderwijs volgt grotendeels dezelfde verwerkingspraktijken als andere basisscholen en neemt de richtlijnen van Kennisnet met betrekking tot DPIA's over. Dit houdt in dat we een DPIA uitvoeren voor verwerkingen die een hoog risico inhouden voor de rechten en vrijheden van betrokkenen. Elke nieuwe gegevensverwerking wordt gemeld aan de Privacy en Security Officer.

#### **7.2.7 Naleving en sancties**

Naleving houdt in dat we dagelijks toezicht houden op de naleving van ons beleid en onze richtlijnen. Leidinggevend en proceseigenaren spelen hierbij een belangrijke rol door hun medewerkers aan te spreken op eventuele tekortkomingen. We besteden actief aandacht aan Informatiebeveiliging en privacy (IBP) via verschillende methoden, zoals bij aanstelling, tijdens functioneringsgesprekken, met behulp van een organisatiebrede gedragscode, en via

periodieke bewustwordingscampagnes. De Functionaris voor Gegevensbescherming (FG) speelt een cruciale rol in het toezicht op de naleving van de AVG en heeft toegang tot de voortgang van het IBP-beleid.

Als de naleving van dit beleid ernstig tekortschiet, kan Stichting Optimus Onderwijs passende sancties opleggen aan de verantwoordelijke medewerkers binnen de kaders van de CAO en de wettelijke mogelijkheden.

### 7.3 Ondersteunende richtlijnen en procedures

Om dit beleid in detail uit te werken, maken we gebruik van verschillende aanvullende beleidsdocumenten, richtlijnen, procedures en protocollen. Deze beheert de Privacy en Security Officer.

Als onderdeel van dit IBP-beleid verwijzen naar onderstaande documenten.

- Beleid voor classificatie, labeling en behandeling van informatie.
- Beleid voor het aanvragen van bedrijfsmiddelen.
- Beleid voor het gebruik van mobiele apparatuur en verwijderbare media.
- Beleid voor het beheer van leveranciersdiensten.
- Naleving van wettelijke en contractuele verplichtingen.

Deze documenten maken allemaal deel uit van dit hoogste niveau beleid en dienen op hetzelfde niveau te worden gehandhaafd.

### 7.4 Technisch beveiligingsbeleid

Het technische beveiligingsbeleid is gericht op het definiëren van het doel, de richting, de principes en de basisregels met betrekking tot informatiebeveiliging binnen de technische omgevingen van Optimus.

Naast dit technische beveiligingsbeleid heeft Optimus ook een algemeen beleid ontwikkeld voor de medewerkers die betrokken zijn.

Het technische beveiligingsbeleid is van toepassing op de scope van het Information Security Management System (ISMS), zoals gedefinieerd in Optimus Informatiebeveiligingsbeleid-document.

### 7.5 Bronvermelding:

Voor de opbouw van dit document hebben we de volgende bronnen geraadpleegd:

- [Aanpak IBP - Aanpak informatiebeveiliging en privacy in het onderwijs \(kennisnet.nl\)](#)
- [Algemeen Informatie Beleid NewDay](#)

## 8. Bijlage 1 | Locaties scholen Stichting Optimus Primair Onderwijs

Onze stichting omvat veertig scholen, waaronder twee SBO-scholen, gelegen in de provincie Noord-Brabant.



|                                                                                |                                                                          |                                                                             |                                                                                      |
|--------------------------------------------------------------------------------|--------------------------------------------------------------------------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| <b>De Akkerwinde</b><br>Berkenkamp 2<br>5434 PD Vianen NB<br>0485 314957       | <b>De Bakelgeert</b><br>Stationsweg 40<br>5831 CR Boxmeer<br>0485 573386 | <b>De Bogaard</b><br>Stationssingel 10<br>5371 BB Ravenstein<br>0486 412236 | <b>De Bolster</b><br>Grotestraat 68<br>5836 AH Sambeek<br>0485 573330                |
| <b>De Bongerd</b><br>Kerkstraat 7<br>5443 AA Haps<br>0485 315385               | <b>De Bongerd</b><br>Schoolstraat 8<br>5438 AC Gassel<br>0486 473462     | <b>De Ester</b><br>Sint Machutusweg 2a<br>5364 RB Escharen<br>0486 472256   | <b>De Klimop</b><br>Wethouder Lindersstraat 81<br>5455 GK Wilbertoord<br>0485 478675 |
| <b>De Kreek'l</b><br>Monseigneur Suijsstraat 6<br>5375 AG Reek<br>0486 420520  | <b>De LenS</b><br>Langenboomseweg 1b<br>5451 JH MILL<br>0485 470150      | <b>De Linde</b><br>Hoogstraat 1<br>5367 AA Macharen<br>0412 492327          | <b>Den Omgang</b><br>Bossestraat 8b<br>5374 HT Schaijk<br>0486 461283                |
| <b>De Raamdonk</b><br>Burgemeester Ficqilaan 4<br>5361 AX Grave<br>0486 729000 | <b>De Regenboog</b><br>Runstraat 16<br>5374 AC Schaijk<br>0486 461365    | <b>De Regenboog</b><br>Eurodreef 1<br>5431 VG Cuijk<br>0485 313429          | <b>De Schare</b><br>Wethouder Lemmenstraat 9<br>5454 GH Sint Hubert<br>0485 470154   |

|                                                                                  |                                                                               |                                                                                                 |                                                                              |
|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>De Sprankel</b><br>Gasthuishoeve 1<br>5361 HT Grave<br>0486 472077            | <b>De Sprong</b><br>Lindenplein 17<br>5446 AV Wanroij<br>0485 470886          | <b>De vier Heemskinderen</b><br>Rondestraat 31<br>5352 LJ Deursen-<br>Dennenburg<br>0486 411521 | <b>De Waai</b><br>Lavendel 2a<br>5432 DH Cuijk<br>0485 311790                |
| <b>De Wegwijzer</b><br>Burgemeester Ficqlaan 4<br>5361 AX Grave<br>0486 729001   | <b>De Weijerwereld</b><br>Weijerstraat 2<br>5831 JV Boxmeer<br>0485 571073    | <b>De Zevensprong</b><br>Dassenburcht 36b<br>5431 JZ Cuijk<br>0485 219005                       | <b>De Zonnewijzer</b><br>Schoolstraat 5<br>5843 AG Westerbeek<br>0485 384248 |
| <b>Dr. Jan De Quay</b><br>WPF Ghijsenstraat 2<br>5437 AP Beers NB<br>0485 315085 | <b>Het Baken</b><br>De Vlasakkers 3<br>5345 BC Oss<br>0412 633805             | <b>Het Telraam</b><br>Kerkstraat Zuid 24<br>5441 AK Oeffelt<br>0485 361622                      | <b>Klimop</b><br>Kerkveld 2<br>5447 AV Rijkevoort<br>0485 371726             |
| <b>Klim Op</b><br>Clarastraat 1<br>5366 AK Megen<br>0412 462311                  | <b>Leander</b><br>Remmensberg 33<br>5845 DD Sint Anthonis<br>0485 381892      | <b>Lindekring</b><br>Liesmortel 19<br>5435 XH Sint Agatha<br>0485 311611                        | <b>Matthias</b><br>Deken Schmerlingstraat 17<br>5841 AM Oploo<br>0485 381839 |
| <b>Onze Bouwsteen</b><br>Moerkamp 73<br>5835 BP Beugen<br>0485 361683            | <b>Palet</b><br>Pastoor Kerstenstraat 38<br>5831 EW Boxmeer<br>0485 571685    | <b>Pater Eymard</b><br>Pater Eymardstraat 8<br>5844 AK Stevensbeek<br>0485 382270               | <b>Sint Jozef</b><br>Beukenlaan 6<br>5363 RA Velp NB<br>0486 422348          |
| <b>Sint Lambertus</b><br>Grotestraat 6<br>5368 AK Haren NB<br>0412 462276        | <b>'t Schrijverke</b><br>Wassenbergstraat 12<br>5373 CH Herpen<br>0486 411828 | <b>'t Stekske</b><br>Dominicanenstraat 22<br>5453 JN Langenboom<br>0486 431303                  | <b>Vlasgaard</b><br>Kerkstraat 57-59<br>5411 EA Zeeland<br>0486 451252       |

