Informatiebeveiligings- en Privacy beleid 2025

Stichting SWV 2505

Opgesteld op 9 december 2025

Inhoud

1 Inleiding 3

1.1. Toelichting informatiebeveiliging en privacy 3

1.2. Toelichting privacy 3

1.3. Vervlechting informatiebeveiliging en privacy 3

2. Doel en reikwijdte 4

2.1. Doel 4

2.2. Reikwijdte 4

3. Uitgangspunten 5

3.1 Algemene beleidsuitgangspunten 5

3.2. Uitgangspunten privacy 5

4. Wet- en regelgeving 6

5. Organisatie 6

6. Controle en rapportage 7

6.1. Ondersteunende richtlijnen en procedures 7

6.2. Voorlichting en bewustzijn 7

6.3. Classificatie en risicoanalyse 7

6.4. Incidenten en datalekken 7

6.5. Naleving en sancties 7

Bijlage 1: Ondersteunende richtlijnen en procedures 10

Bijlage 2: IBP rollen en taken 11

1. Inleiding

Het Samenwerkingsverband (SWV 2505) is t.b.v. de uitvoering van haar wettelijke taken afhankelijk van informatie en informatieoverdracht. De hoeveelheid privacygevoelige informatie en de wijze waarop wij deze informatie delen noodzaakt ons om deze informatie optimaal te beschermen en veilig en verantwoord met persoonsgegevens om te gaan.

Het is van belang om adequate maatregelen te nemen op het gebied van informatiebeveiliging en privacy om de gevolgen van mogelijke risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het SWV en de bedrijfsvoering optimaal te kunnen waarborgen.

1.1 Toelichting informatiebeveiliging en privacy

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.

Informatiebeveiliging richt zich op de volgende aspecten:

- **Beschikbaarheid:** de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- **Integriteit:** de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- **Vertrouwelijkheid:** de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het passend onderwijsproces en bij de bedrijfsvoering van het SWV. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

1.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt o.a. onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:

Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige

andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

1.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk. Het onderwerp informatiebeveiliging en privacy wordt afgekort tot IBP. Dit beleid vormt de basis voor de aanpak binnen het SWV.

2. Doel en reikwijdte

2.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

➢ Het waarborgen van de continuïteit van het SWV en de bedrijfsvoering.

➢ Het garanderen van de privacy van leerlingen en medewerkers, waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.

Het informatiebeveiligings- en privacy beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en het SWV voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het IBP-beleid geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het netwerk verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen het SWV, waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan het SWV persoonsgegevens verwerkt.
- Het IBP-beleid geldt voor de verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van het SWV evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- IBP-beleid heeft binnen het SWV raakvlakken met:
    - *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen.

- *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
- *IT-beleid;* met als aandachtspunten beheer en gebruik van ICT en (digitale) leermiddelen.
- *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers in de OPR en MRP.

3. Uitgangspunten

3.1 Algemene beleidsuitgangspunten

1. Informatiebeveiliging en privacy voldoet aan alle relevante wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming.
2. De verwerking van persoonsgegevens is altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van het SWV om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen te allen tijde hun toestemming herzien.
3. Binnen het SWV is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie maar ook van papieren documenten.
4. Het SWV heeft als rechtspersoon zeggenschap over de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert het SWV informatie waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
5. Het SWV sluit met alle leveranciers van digitale services (zowel van educatieve - als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van het SWV, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
6. Het SWV kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy zodat tijdig de juiste maatregelen genomen kunnen worden.
7. Het SWV neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's die de voortgang van passend onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.

8. Het SWV zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

3.2 Uitgangspunten privacy

De vijf vuistregels m.b.t. de omgang van persoonsgegevens bij het SWV zijn:

9. **Doelbepaling en doelbinding:** persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
10. **Grondslag:** verwerking van persoonsgegevens is gebaseerd op één van de zes wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene of een gerechtvaardigd belang.
11. **Dataminimalisatie:** bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiair). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
12. **Data-integriteit:** er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

4. Wet- en regelgeving

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

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra.
- Wet goed onderwijs en goed bestuur PO/VO.
- Wet onderwijstoezicht.
- Algemene Verordening Gegevensbescherming.
- Archiefwet.
- Leerplichtwet.
- Auteurswet.
- Wetboek van Strafrecht.

5. Organisatie

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierin spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Hieronder wordt beschreven hoe IBP in het SWV is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

Richtinggevend

Eindverantwoordelijke

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

Sturend

Directeur

De directeur geeft terugkoppeling en advies aan de eindverantwoordelijke (bestuur) en stuurt de mensen aan op uitvoerend niveau. De directeur moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling.
- De uniformiteit bewaken.
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy.
- De verdere afhandeling van incidenten coördineren.
- De toepassing en werking van het IBP-beleid op basis van regelmatige rapportages evalueren.

Functionaris voor Gegevensbescherming

De Functionaris voor Gegevensbescherming (FG) houdt binnen het SWV toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze Functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het verbeteren en stimuleren van bewustwording rondom IBP, het afhandelen van informatiebeveiligingsincidenten, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het bestuur).

Uitvoerend

Medewerker

Alle medewerkers hebben in hun dagelijkse werkzaamheden verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy.

6. Controle en rapportage

Het IPB-beleid wordt jaarlijks geactualiseerd.

6.1 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

6.2 Voorlichting en bewustzijn

Het IBP-bewustzijn is de verantwoordelijkheid van het bestuur.

6.3 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn. Informatie wordt alleen gedeeld en opgeslagen op de daarvoor bestemde systemen.

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde

verwerkingen op informatiebeveiliging en privacy zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ICT)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

6.4 Incidenten en datalekken

Alle medewerkers die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol.

De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings-)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings-)incidenten kunnen worden gemeld bij info@swv-vo-2505.nl.

6.5 Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat het bestuur verantwoordelijkheid neemt en de medewerkers aanspreekt in geval van tekortkomingen.

Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

6.6 ICT

Voor het gebruik van ICT-middelen geldt dat deze altijd beheerd en geconfigureerd worden door dienstleveranciers met voldoende kennis zodat SWV voldoet aan de geldende wet- en regelgeving. De dienstleverancier zorgt dat alle gebruikte ICT bekend is en onderdeel is van het incidentmanagement-proces. Ook voldoet de ICT-dienstverlener aan hoge security management standaarden, waarbij SWV te allen tijde inzicht kan krijgen in de status en werking van:

- **Beveiligingsbaselines –** Er zijn uniforme en up-to-date beveiligingsstandaarden voor systemen en applicaties.
- **Authenticatiemechanismes –** Er worden passende authenticatiemethoden toegepast om veilige toegang te waarborgen.
- **Mobiele apparaten en telewerken –** Er zijn maatregelen om veilige toegang en gebruik van mobiele apparaten en externe werkplekken te garanderen.
- **Logging systeemactiviteiten –** Systeemactiviteiten worden gelogd en gemonitord om afwijkingen en beveiligingsincidenten te detecteren.
- **Patchmanagement –** Beveiligingsupdates en patches worden tijdig geïmplementeerd om kwetsbaarheden te minimaliseren.
- **Threat- en vulnerabilitymanagement –** Dreigingen en kwetsbaarheden worden proactief geïdentificeerd, beoordeeld en aangepakt.
- **Beschikbaarheid en bescherming infrastructuur –** De IT-infrastructuur wordt adequaat beschermd en beschikbaarheid is gewaarborgd.
- **Onderhoud van de infrastructuur –** Regelmatig onderhoud en updates zorgen voor een stabiele en veilige infrastructuur.
- **Cryptografisch sleutelmanagement –** Beheer en bescherming van cryptografische sleutels voldoen aan best practices.
- **Netwerkbeveiliging –** Netwerkverkeer wordt beveiligd door passende maatregelen zoals firewalls en segmentatie.
- **Beheersing van malware-aanvallen –** Er zijn effectieve maatregelen om malware te detecteren, voorkomen en bestrijden.

- **Bescherming van beveiligingstechnologie –** Beveiligingsoplossingen worden onderhouden en beschermd tegen manipulatie of uitval.

6.7 Changemanagement

Wijzigingen bij de ICT-dienstverlener worden doorgevoerd volgens een formeel en gedocumenteerd proces. Kritieke wijzigingen vereisen voorafgaande goedkeuring van SWV en een gedegen impactanalyse. Communicatie met belanghebbenden zorgt voor transparantie terwijl monitoring en evaluatie waarborgen dat wijzigingen effectief en zonder verstoringen worden doorgevoerd.

6.8 Identity & Acces Management

De ICT-dienstverlener beheert wijzigingen in het personeelsbestand binnen Identity & Access Management (IAM). Nieuwe medewerkers krijgen tijdig de juiste toegangsrechten terwijl vertrekkende of veranderende medewerkers snel worden aangepast of verwijderd. Toegangsrechten worden bij wijzigingen in het personeelsbestand opnieuw geëvalueerd.

6.9 Continuïteit

SWV waarborgt continuïteit doordat haar ICT-dienstleverancier voldoende back-up maatregelen heeft getroffen waardoor maximaal gegevensverlies niet meer is dan 1 dag.

Bijlage 1: Ondersteunende richtlijnen en procedures

Documenten:

Procesbeschrijving melden datalekken.

Registratie beveiligingsincidenten.

Dataregister om te voldoen aan de registratieplicht.

Verwerkersovereenkomsten.

Functionaris voor Gegevensbescherming.

Bijlage 2: IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Bestuur	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid
Sturend (tactisch)	Directeur	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur over IBP • Voorbereiden uitvoeren IBP-beleid, classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	• Beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Gedragscode ICT en internetgebruik • Gedragscode medewerkers en leerlingen • Privacy protocol • Verwerkersovereenkomsten
	Functionaris voor Gegevensbescherming	• Toezicht op naleving privacy wetgeving	• Privacyreglement • Procedure IBP-incident afhandeling

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
		• Voorlichting privacy en stimuleren bewustwording • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Inrichten meldpunt datalekken
Uitvoerend (operationeel)	Medewerker Dagelijkse leiding/ leidinggevende/ bestuur	**Communiceren, informeren en toezien op naleving van o.a.:** • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden • Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid • Implementeren IBP-maatregelen • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur	• IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media