



Stichting PrimAH

Beleid Informatie Beveiliging & Privacy



Inhoud

Inhoud	2
Inleiding	3
Toelichting informatiebeveiliging en privacy	4
Toelichting informatiebeveiliging	4
Toelichting privacy	4
Vervlechting informatiebeveiliging en privacy	4
Doel en reikwijdte	5
Doel	5
Reikwijdte	5
IBP uitgangspunten bij Stichting PrimAH	7
Uitwerking van het beleid – Wat doen we?	9
Relevante wet- en regelgeving	9
Basisregels bij het omgaan met persoonsgegevens	9
Ondersteunende richtlijnen en procedures	10
Voorlichting en bewustzijn	10
Classificatie en risicoanalyse	10
Incidenten en datalekken	10
Planning en controle	11
Naleving en sancties	11
Logging en monitoring	11
Organisatie - Wie doet wat?	12
Rollen en verantwoordelijkheden	12
Bijlage 1: Ondersteunende richtlijnen en procedures	14
Bijlage 2: Organisatie	17
Richtinggevend	17
Sturend	17
Uitvoerend	18

Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

Dit stuk vormt de kapstok voor onderliggend beleid en procedures. In bijlage 1 is een overzicht opgenomen met de aanhangige procedures en een uitleg van de inhoud.

Toelichting informatiebeveiliging en privacy

Toelichting informatiebeveiliging

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 onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere 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.

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, en worden daarom samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen Stichting PrimAH te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

Doel en reikwijdte

Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- ✓ Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- ✓ Het garanderen van de privacy van alle betrokkenen waarvan Stichting PrimAH persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers
- ✓ Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er 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 Stichting PrimAH voldoet aan relevante wet- en regelgeving.

Reikwijdte

- ✓ Het IBP-beleid binnen Stichting PrimAH geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers, vrijwilligers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- ✓ Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting PrimAH waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers, vrijwilligers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Stichting PrimAH persoonsgegevens verwerkt.
- ✓ Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Stichting PrimAH. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.)
- ✓ Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Stichting PrimAH 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 Stichting PrimAH 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
- ✓ *ICT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen
- ✓ *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers

IBP uitgangspunten bij Stichting PrimAH

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

- ✓ Het bestuur van Stichting PrimAH neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
- ✓ Stichting PrimAH voldoet aan alle relevante wet- en regelgeving.
- ✓ Bij Stichting PrimAH is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Stichting PrimAH om persoonsgegevens te verwerken en het belang van betrokkenen om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van hun persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien.
- ✓ Stichting PrimAH informeert alle betrokkenen helder en actief over de verwerkingen van hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.
- ✓ Stichting PrimAH legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Stichting PrimAH voldoet hiermee aan de documentatieplicht.
- ✓ Binnen Stichting PrimAH 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.
- ✓ Stichting PrimAH is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheren de scholen informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
- ✓ Stichting PrimAH classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.

- ✓ Stichting PrimAH sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
- ✓ Stichting PrimAH verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagooverlies. Stichting PrimAH heeft hiervoor privacy-, ICT-gebruiks- en Social mediareglementen opgesteld en geïmplementeerd.
- ✓ Informatiebeveiliging en privacy is bij Stichting PrimAH een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- ✓ Stichting PrimAH 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.
- ✓ Stichting PrimAH neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.
- ✓ Indien de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt Stichting PrimAH aanvullende afspraken vast over de technische maatregelen.
- ✓ Stichting PrimAH legt alle beveiligingsincidenten en datalekken vast volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen

Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

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 en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- ✓ Wet goed onderwijs en goed bestuur PO/VO
- ✓ Wet onderwijstoezicht
- ✓ Algemene Verordening Gegevensbescherming (AVG)
- ✓ Archiefwet
- ✓ Leerplichtwet
- ✓ Auteurswet
- ✓ Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

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:** 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.
2. **Grondslag:** verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.
3. **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 (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie:** de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit:** er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

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.

Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP en de FG met het bestuur van Stichting PrimAH als eindverantwoordelijke.

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.

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.

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 procedure. 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 de manager IBP via privacy@primah.org.

Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
- de actuele geïnventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan.

Daarnaast kent Stichting PrimAH een jaarlijkse planning- en controlcyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

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 leidinggevend en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instellingsbrede gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door Stichting PrimAH vast te stellen reglement.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan Stichting PrimAH de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt er voor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging tot) ongeautoriseerde toegang tot het netwerk.

Organisatie - Wie doet wat?

Rollen en verantwoordelijkheden

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. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij Stichting PrimAH.

Niveau	Wie	Hoe	Wat
	Rollen	Verantwoordelijkheid / taken	Realiseren / vastleggen
Richtinggevend (strategisch)	Bestuur Stichting PrimAH	- 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 - Baseline / basismaatregelen - Reglement FG vaststellen - Privacyreglement vaststellen 2-jaarlijks updaten IBP-beleid
Sturend (tactisch)	Manager IBP	- Inhoudelijk verantwoordelijk voor IBP - Algemeen aanspreekpunt IBP - IBP-planning en controle - Adviseert bestuur/CvB/directie 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	Processen, richtlijnen en procedures IBP, waaronder: - activiteitenkalender - Protocol beveiligingsincidenten en datalekken - Verwerkersovereenkomsten regelen - Brief toestemming gebruik beeldmateriaal - Opstellen informatie documentatie richting leerlingen, ouders / verzorgers - Security awareness activiteiten - Sociale media reglement - Gedragscode ICT en internetgebruik - Gedragscode medewerkers en leerlingen Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: - Toegangsmatrix diverse informatiesystemen en netwerk - Beheer dataregister
	Functionaris voor Gegevensbescherming	- Toezicht op naleving privacy wetgeving - Voorlichting privacy en stimuleren bewustwording - Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde	- Privacyreglement, - procedure IBP-incident afhandeling - Inrichten meldpunt datalekken

		bescherming van verwerkingen van persoonsgegevens Afwikkeling klachten en incidenten	
	Domeinverantwoordelijke proceseigenaren: Stafbureau PIT PET Administratie	Classificatie / risicoanalyse in samenwerking met Manager IBP - Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur. - Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. - Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	- Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister - Classificatie- en risicoanalyse documenten.
Uitvoerend (operationeel)	Medewerker	Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	Communiceren, informeren en toezien op naleving van o.a.: - IBP in het algemeen - Regels passend onderwijs - Hoe omgaan met leerling dossiers - Wie mogen wat zien - Gedragscode - Omgaan met sociale media - Mediawijs maken
	Directie	- Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. - Toezen 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. - periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; - Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	

De verdere uitwerking van de rollen en taken staan beschreven in bijlage 2.

Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een overzicht van een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Aan dit document zijn toegevoegd:

Document	Inhoud
Privacyreglement – Medewerkers	<i>Beschrijving van de afspraken rond de verwerking van persoonsgegevens van medewerkers binnen Stichting PrimAH.</i>
Privacyreglement – Leerlingen	<i>Beschrijving van de afspraken rond de verwerking van persoonsgegevens van (ouders van) leerlingen binnen Stichting PrimAH.</i>
ICT-gebruiksreglement – Medewerkers	<i>Beschrijving van de afspraken rond het gebruik van ICT-middelen en –systemen door medewerkers van Stichting PrimAH.</i>
ICT-gebruiksreglement – Leerlingen	<i>Beschrijving van de afspraken rond het gebruik van ICT-middelen en –systemen door leerlingen van Stichting PrimAH.</i>
Social media reglement – Medewerkers	<i>Beschrijving van de afspraken rond het gebruik van sociale media door medewerkers van Stichting PrimAH.</i>
Social media reglement – Leerlingen	<i>Beschrijving van de afspraken rond het gebruik van ICT-middelen en –systemen door (ouders van) leerlingen van Stichting PrimAH.</i>
Procedure – Extern delen beeldmateriaal	<i>Deze procedure beschrijft de gang van zaken bij het extern publiceren van beeldmateriaal. Naast de uitgangspunten voor het publiceren, voorziet deze procedure in een uitgebreide beschrijving hoe het verkrijgen van toestemming binnen Stichting PrimAH is geregeld.</i>
Procedure – Intern gebruik beeldmateriaal	<i>Deze procedure beschrijft de gang van zaken bij het gebruik van beeldmateriaal binnen Stichting PrimAH.</i>
Procedure – Cameratoezicht	<i>Deze procedure beschrijft de gang van zaken rond het uitvoeren van cameratoezicht in en om de gebouwen van Stichting PrimAH.</i>

Procedure – Melden beveiligingsincidenten	<i>Deze procedure beschrijft de gang van zaken bij het intern en extern melden van beveiligingsincidenten, waaronder datalekken.</i>
Procedure – Bewaarbeleid	<i>Deze procedure beschrijft de gang van zaken rond het bewaren en vernietigen van persoonsgegevens.</i>
Procedure – Inzien van schoolwerk en toetsen	<i>Deze procedure beschrijft de gang van zaken rond het inzien van schoolwerk en gemaakte toetsen door ouders van leerlingen.</i>
Procedure – Rechten betrokkenen	<i>Deze procedure beschrijft de gang van zaken rond de uitoefening van de rechten van betrokkenen met het oog op de AVG.</i>
Procedure – Responsible Disclosure	<i>Deze procedure beschrijft de gang van zaken wanneer een beveiligingslek wordt ontdekt door een externe in de systemen van Stichting PrimAH.</i>

Naast de geldende procedures maakt Stichting PrimAH gebruik van een aantal ‘lopende’ documenten. Deze hoeven niet te worden vastgesteld, maar zijn (indien de situatie zich hiervoor leent, te beoordelen door FG) vrij inzichtelijk.

Document	Inhoud
Dataregister	<i>In het dataregister houdt Stichting PrimAH de verwerkingen van persoonsgegevens bij. Naast de verwerkingen, worden de gegevens en systemen in dit register geclassificeerd op risico.</i>
Autorisatiematrix	<i>De autorisatiematrix voor Stichting PrimAH geeft een overzicht van de toegangsrechten van diverse functiegroepen binnen de organisatie.</i>
Incidentenregister*	<i>In dit register worden beveiligingsincidenten bijgehouden.</i>
Verwerkersovereenkomsten	<i>Stichting PrimAH sluit met diverse partijen verwerkersovereenkomsten af. Deze overeenkomsten worden op een centrale plek bewaard. Een overzicht van de afgesloten overeenkomsten is (op aanvraag) beschikbaar voor alle betrokkenen.</i>
DPIA overzichten	<i>De overzichten van de DPIA geven inzicht in de uitkomsten van de diverse risicoanalyses binnen de organisatieonderdelen.</i>

Diverse communicatie informeren betrokkenen

De diverse in- en uitgaande communicatie naar betrokkenen wordt gearhiveerd. Dit archief is op aanvraag inzichtelijk.

**het incidentenregister is niet in zijn geheel openbaar inzichtelijk. Bij een verzoek tot inzage beoordeelt de FG welke informatie noodzakelijk is voor het verschaffen van helderheid.*

Bijlage 2: Organisatie

Deze bijlage beschrijft hoe IBP op drie niveaus wordt georganiseerd.

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

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

Beschreven wordt welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Richtinggevend

Eindverantwoordelijke

Het bestuur van Stichting PrimAH 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 ligt bij de manager IBP.

Sturend

Manager IBP

Manager IBP 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 manager IBP moet:

- ✓ Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling;
- ✓ De uniformiteit bewaken binnen Stichting PrimAH;
- ✓ Het aanspreekpunt zijn voor vragen of bij incidenten op het gebied van informatiebeveiliging en privacy;
- ✓ De verdere afhandeling van incidenten binnen Stichting PrimAH coördineren.

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt binnen Stichting PrimAH 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). De FG heeft regelmatig overleg met manager IBP. De FG is ook de contactpersoon voor klachten van betrokkenen.

PrimAH ICT Team

Adviseert samen met manager IBP (of informatiemanager) de eindverantwoordelijke en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen Stichting PrimAH.

Domeinverantwoordelijke / proceseigenaar

Binnen de organisatie zijn er verschillende domeinen/processen, zoals ict, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Deze proceseigenaar is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:

- ✓ Samen met de manager IBP stellen zij het beleid voor toegang (autorisaties) vast.
- ✓ Samen met functioneel beheer en ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- ✓ Samen met functioneel beheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

Uitvoerend

Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

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

Directie

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- ✓ er voor te zorgen dat zijn medewerkers op de hoogte zijn van het IBP-beleid;
- ✓ toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- ✓ periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- ✓ als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de manager IBP. Leidinggevendens hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.