

Informatiebeveiligings- en privacy beleid

Stichting Ambion



Versiebeheer

Datum	Auteur	Versie	Status	Aanpassing
	A. Dijk	1.0	Concept	

Vastgesteld door Stichting Ambion.

Het informatiebeveiligings- en privacy beleid is aangepast aan de eisen en termen vanuit de AVG. Elke organisatie moet niet alleen de privacywetgeving naleven, maar moet ook aantoonbaar voldoen aan de AVG.

Bij het template hoort een document met dezelfde inhoud, maar dan voorzien van een aparte toelichting. Die toelichting bevat verdere uitleg en verwijzingen naar onderliggende documenten, afspraken en procedures. Hiermee wordt de 'kapstokfunctie' van het beleid inzichtelijker.

Bron

Kennisnet

Bewerkt door:

Stichting Ambion

INHOUD:

1	HET BELANG VAN INFORMATIEBEVEILIGING EN PRIVACY	3
2	TOELICHTING INFORMATIEBEVEILIGING EN PRIVACY	3
2.1	TOELICHTING INFORMATIEBEVEILIGING	3
2.2	TOELICHTING PRIVACY	3
2.3	VERVLECHTING INFORMATIEBEVEILIGING EN PRIVACY	3
3	DOEL EN REIKWIJDTE	4
3.1	DOEL	4
3.2	REIKWIJDTE	4
4	BELEID – HOE DOEN WE DAT?	4
5	UITWERKING VAN HET BELEID – WAT DOEN WE?	6

5.1	RELEVANTE WET- EN REGELGEVING.....	6
5.2	BASISREGELS BIJ HET OMGAAN MET PERSOONSgegevens.....	6
5.3	ONDERSTEUNENDE RICHTLIJNEN EN PROCEDURES	7
5.4	VOORLICHTING EN BEWUSTZIJN.....	7
5.5	CLASSIFICATIE EN RISICOANALYSE.....	7
5.6	INCIDENTEN EN DATALEKKEN	7
5.7	PLANNING EN CONTROLE	7
5.8	NALEVING EN SANCTIES	7
5.9	LOGGING EN MONITORING	8
6	ORGANISATIE - WIE DOET WAT?	9
6.1	ROLLEN EN VERANTWOORDELIJKHEDEN	9
	BIJLAGE 1: ONDERSTEUNENDE RICHTLIJNEN EN PROCEDURES.....	11
	BIJLAGE 2: ORGANISATIE; WIE DOET WAT.....	12

1 Het belang van informatiebeveiliging en privacy

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.

2 Toelichting informatiebeveiliging en privacy

2.1 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 imagooverlies.

2.2 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.

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

Binnen Stichting Ambion realiseren wij ons dat er soms een spanningsveld kan ontstaan tussen gebruiksgemak en informatiebeveiliging. Binnen dit spanningsveld zoeken wij de meest passende oplossing, binnen de kaders van de AVG wet- en regelgeving.

3 Doel en reikwijdte

3.1 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 Ambion 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 Ambion voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen Stichting Ambion 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 schoolnetwerk verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting Ambion waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Stichting Ambion persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Stichting Ambion. 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 Ambion 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 Ambion 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 aanschaf, beheer en gebruik van ict en (digitale) leermiddelen;
 - *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers.

4 Beleid – Hoe doen we dat?

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

1. Het schoolbestuur van Stichting Ambion neemt de verantwoordelijkheid om ervoor te zorgen dat in-

formatiebeveiliging 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.

2. Stichting Ambion voldoet aan alle relevante wet- en regelgeving.
3. Bij Stichting Ambion 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 Ambion 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 ten alle tijden hun toestemming herzien.
4. Stichting Ambion zal alle betrokkenen helder en actief informeren 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.
5. Stichting Ambion legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Stichting Ambion voldoet hiermee aan de documentatieplicht.
6. Binnen Stichting Ambion 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.
7. Stichting Ambion is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. Stichting Ambion 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.
9. Stichting Ambion 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.
10. Stichting Ambion 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 imago-verlies. Stichting Ambion heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy is bij Stichting Ambion een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. Stichting Ambion 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.
13. Stichting Ambion 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.
14. Stichting Ambion zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol

afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen

5 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.

5.1 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
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- 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.

5.2 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:** 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 ongevroegd 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.

5.3 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.

5.4 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 projectleider IBP, de FG, en de Privacy Officer met het bestuur als eindverantwoordelijke.

5.5 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 (d.m.v. een zgn. DPIA). Vanaf de start van nieuwe (ICT)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

5.6 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 dienen te worden gemeld via het formulier op de openbare Ambion website of de Privacypagina op Intranet. Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.7 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 Ambion een jaarlijkse planning en control cyclus 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.

5.8 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 medewer-

kers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede 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 de het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan Stichting Ambion de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.9 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgen ervoor 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.

6 Organisatie - Wie doet wat?

6.1 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.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid/ taken	Wat Realiseren/ vastleggen
Richtgevend (strategisch)	College van 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 - Baseline/ basismaatregelen - Reglement FG vaststellen - Privacyreglement vaststellen
Sturend (tactisch)	Projectleider IBP	- Inhoudelijk verantwoordelijk voor 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
	Functionaris voor Gegevensbescherming en/of Privacy Officer	- Toezicht op naleving privacywetgeving - Voorlichting privacy en stimuleren bewustwording - Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens - Afwikkeling klachten en incidenten	- Privacyreglement, - Procedure IBP-incident afhandeling - Inrichten meldpunt datalekken
	Domeinverantwoordelijke/ Proceseigenaren Waaronder o.a.: - ICT-beheer, - HRM/ P&O, - Facilitair, - Onderwijs, - Financiën, - Inkoop en administratie	Classificatie/ risicoanalyse in samenwerking met Projectleider IBP/ Privacy Officer) Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/CvB/directie - Samen met functioneel beheer en ICT-beheer erop 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	- Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister - Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: - Toegangsmatrix diverse informatiesystemen en netwerk

		gebruikers regelmatig beoordelen en controleren.	
Uitvoerend (operationeel)	IBP-Team	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten.	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
	Applicatie beheerder	• Uitvoeren taken conform gegeven richtlijnen en procedures.	
	Medewerker	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	
	Dagelijkse leiding/ leiding-gevende/ directie	• Communicatie naar alle betrokkenen; ervoor 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. • Periodiek het onderwerp informatie-beveiliging 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 aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Documenten:

Procedure toestemming gebruik beeldmateriaal
 Procedure voor verwijderen van gegevens
 Communicatierechten betrokkenen
 Procesbeschrijving rechten betrokkenen
 Privacyreglement
 Autorisatiematrix
 Afspraken gebruik sociale media
 Procedure rondom training medewerkers
 Cameratoezicht
 Wachtwoordbeleid
 Responsible disclosure
 Gedragscode ict en internetgebruik
 Acceptable use policy
 Procedure rondom uitwisselen gegevens

Aandachtspunten:

(toestemmingsbrief)
 (bewaartermijnen)
 (communicatie richting betrokkenen)
 (proces rondom aanvragen van betrokkenen)

 (wie mogen gegevens inzien, bewerken enz.)

 (bewustzijn creëren)

 (verantwoord gebruik bedrijfsmiddelen)
 (passend onderwijs, leerling dossiers, leerplicht enz)

Verplicht vanuit de AVG:

Procesbeschrijving melden datalekken
 Registratie beveiligingsincidenten
 Dataregister om te voldoen aan de registratieplicht
 Verwerkersovereenkomsten
 Procedure gegevensbeschermingseffectbeoordeling
 Risicoanalyse
 Functionaris voor Gegevensbescherming

(privacy bijlage beschikbaar stellen)
 (DPIA)

 (communicatie hierover richting medewerkers)

Bijlage 2: Organisatie; wie doet wat

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 Ambion 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 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 projectleider IBP.

Sturend

Projectleider IBP

Projectleider 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 Projectleider IBP moet:

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

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt binnen Stichting Ambion 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 de Projectleider IBP. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

ICT-beheer (intern of extern)

Adviseert samen met Projectleider IBP de eindverantwoordelijke en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen Stichting Ambion.

Domeinverantwoordelijke/ proceseigenaar

Binnen de school zijn er verschillende domeinen/processen, zoals ict, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs etc.. 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 eindverantwoordelijke stellen zij het beleid voor toegang (autorisaties) vast;
- Samen met applicatiebeheer en ICT-beheer zien zij erop 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 applicatiebeheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

Uitvoerend

Privacy Officer (PO)

De Privacy Officer vormt een technisch en inhoudelijk aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het personeelshandboek en de handleiding acceptabel gebruikmaken van bedrijfsmiddelen. 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)

Leidinggevende

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

- Ervoor 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.

IBP-team

Het IBP-team wordt organisatie breed zowel preventief als curatief benoemd voor informatiebeveiliging en privacy incidenten. De leden van het AVG -team zijn benoemd door de eindverantwoordelijke en handelen in diens opdracht.

Het IBP-team van Stichting Ambion heeft de volgende opdracht:

- Het signaleren en registreren van alle privacy verzoeken, beveiligingsincidenten en datalekken. Het coördineren van de maatregelen en het toezien op de oplossing van problemen die tot incidenten hebben geleid of waardoor de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;
- Het leveren van managementrapportages en verbetervoorstellen aan de domeinverantwoordelijke/proceseigenaren over de beveiligingsincidenten en verzoeken tot uitoefening privacyrechten van de betrokkenen.

Bij een calamiteit kan het AVG -team terstond bij elkaar worden geroepen op initiatief van de Projectleider IBP, in opdracht van Stichting Ambion. Het doel hiervan is om de **continuïteit** van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:

- Datalek;
- Grote verstoringen van het netwerk (bijvoorbeeld een Phishing- of Ransomware aanval);
- Natuurrampen (brand, overstrooming, storm, etc.).

Het IBP-team bij Stichting Ambion behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.

De werkzaamheden van het IBP-team bij Stichting Ambion is gedocumenteerd en door de eindverantwoordelijke bekrachtigd.