

Informatiebeveiligings- en privacy (IBP) beleid

April 2021

Versiebeheer

Vastgesteld door: Albeda College van Bestuur

Versie	Datum	Naam	Functie
1.0	17-04-2021	Karel Rijkse	Directeur ICT

Het vastgestelde IBP-beleid wordt in PDF formaat op Sharepoint gepubliceerd en voor alle medewerkers en studenten beschikbaar gesteld.

1. Management samenvatting

1.1. Doelstelling

Het Informatiebeveiliging en Privacy (IBP) beleid biedt het kader voor de te nemen maatregelen om:

- De beschikbaarheid van informatie te waarborgen;
- De integriteit van informatie te verzekeren;
- De vertrouwelijkheid van informatie en daarmee de privacy te garanderen.

Met dit IBP beleid geeft het College van Bestuur aan dat zij informatiebeveiliging en privacy belangrijk vindt en biedt zij een basis voor verdere maatregelen en afspraken op het gebied van informatiebeveiliging en privacy binnen Albeda.

1.2. Uitgangspunten en reikwijdte

Het IBP beleid is opgesteld vanuit een werkbare Albeda visie, maar vooral ook vanuit wet en regelgeving op het gebied van privacy (AVG). Binnen Albeda is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Informatiebeveiliging en privacy is bij Albeda een continu proces dat inspeelt op de ontwikkelingen en bedreigingen die op Albeda afkomen. Albeda voldoet aan de relevante wet- en regelgeving en communiceert de maatregelen, maar ook de incidenten, zo helder en open als mogelijk.

1.3. Uitwerking

Voor de relevante IBP maatregelen maakt Albeda gebruik van het raamwerk "IBP in het MBO" dat is opgesteld door de regiegroep "IBP in het MBO" (Kennisnet, SURF en saMBO-ICT). Dit raamwerk wordt door bijna alle MBO instellingen gebruikt en is in overeenstemming met het doel, de uitgangspunten en de reikwijdte van het IBP beleid.

1.4. Organisatie

Binnen Albeda ligt de eindverantwoordelijkheid voor informatiebeveiliging en privacy bij het CvB, ook in de wetgeving (AVG) is vastgelegd dat het bestuur en/of directie eindverantwoordelijk zijn. Naast de rol van het CvB is er binnen Albeda een Regiegroep IBP onder voorzitterschap van de directeur Finance & Control. Daarnaast worden de volgende rollen onderkend binnen de organisatie voor de uitvoering van het IBP beleid:

- Manager informatiebeveiliging / Chief Information Security Officer (CISO) : gedelegeerd sturend verantwoordelijk voor Informatie Beveiliging;
- Functionaris Gegevensbescherming (FG): toezichhouder en gedelegeerd uitvoerend verantwoordelijk voor Privacy;
- Domein verantwoordelijken en proces eigenaren: bepalen samen welke rechten medewerkers krijgen;
- Information Security Officer (ISO): operationeel verantwoordelijk voor het IBP beleid en uitvoer van het IBP plan;
- Dagelijkse leiding en college directie: uitvoerend verantwoordelijk voor IBP;
- Inkoop en juridisch: uitvoerend verantwoordelijk voor verwerkingsovereenkomsten en juridische aansprakelijkheid.

1.5. Voorlichting en bewustzijn

Educatie, training en voorlichting op het gebied van informatiebeveiliging en privacy zijn zeer belangrijk en tevens in de wet vastgelegd (art. 39 lid 1 sub b AVG). Het verhogen van het bewustzijn is een gezamenlijke verantwoordelijkheid van de CISO, de FG en de ISO met het College van Bestuur als eindverantwoordelijke.

Inhoudsopgave

1.	Management samenvatting	3
1.1.	Noodzaak en doel	3
1.2.	Uitgangspunten en reikwijdte	3
1.3.	Uitwerking	3
1.4.	Organisatie	3
1.5.	Voorlichting en bewustzijn	3
2.	Waarom Informatiebeveiliging en privacy	5
3.	Doel, uitgangspunten en reikwijdte	6
3.1.	Doel	6
3.2.	Uitgangspunten	6
3.3.	Reikwijdte	7
4.	Uitwerking	8
4.1.	Informatie Beveiliging Plan (IBP)	8
4.2.	Raamwerk "IBP in het MBO"	8
4.3.	Waar richten we ons op?	8
4.4.	Uitwerking controle maatregelen	8
5.	Organisatie – wie doet wat?	9
5.1.	Rollen en verantwoordelijkheden	9
6.	Rapportage	11
7.	Voorlichting en bewustzijn	12
8.	Toelichting informatiebeveiliging	13
8.1.	Toelichting privacy	13
8.2.	Relevante wet- en regelgeving	13
8.3.	Basisregels voor het omgaan van persoonsgegevens	13
8.4.	Ondersteunende richtlijnen en procedures	14
8.5.	Classificatie en risicoanalyse	14
8.6.	Incidenten en datalekken	14
8.7.	Planning en controle	14
8.8.	Naleving en sancties	14
8.9.	Logging en monitoring	15

2. Waarom Informatiebeveiliging en privacy

De aanleiding voor een informatiebeveiligingsbeleid & privacybeleid komt voort uit de toenemende mate van afhankelijkheid van informatie en ICT in de ondersteuning van de bedrijfsprocessen, niet alleen voor de processen van bestuur en beheer maar met name ook voor het onderwijsproces zelf. Informatiebeveiliging en Privacy zijn belangrijke middelen om de risico's op verstoring van de bedrijfsprocessen en aansprakelijkheid en imagoschade als gevolg van incidenten te voorkomen of te beperken.

Bij informatiebeveiliging gaat het om Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) van gegevens en systemen. Hoe meer eisen er worden gesteld aan de beschikbaarheid, integriteit en vertrouwelijkheid van informatiesystemen hoe meer maatregelen er genomen moeten worden. Om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatiesystemen te waarborgen, is er niet alleen sprake van technologische maatregelen maar is er ook sprake van organisatorische, procesmatige en gedragsmatige maatregelen. Het Informatiebeveiligingsbeleid richt zich op al deze aspecten.

Bij Albeda worden steeds meer persoonsgegevens verwerkt. Hierbij is het van groot belang om heel helder te hebben wat er met die informatie gebeurt en op welke wijze die wordt gebruikt. Het is, op basis van de huidige wetgeving vanuit de Europese Commissie, zaak om hier heel bewust mee om te gaan en adequate maatregelen te treffen om misbruik van persoonsgegevens in het onderwijs te voorkomen. Het Privacy-beleid richt dus specifiek op de vertrouwelijkheid en integriteit binnen Informatiebeveiliging en de wetgeving op dit gebied is vastgelegd in de Algemene Verordening Gegevensbescherming (AVG).

Informatiebeveiliging beleid en Privacy beleid kunnen dus goed samengevoegd worden in het IBP-beleid. Dit IBP-beleid is de basis van informatiebeveiliging en privacy binnen Albeda en vormt de kapstok voor de onderliggende afspraken en procedures.

3. Doel, uitgangspunten en reikwijdte

3.1. Doel

Het Informatiebeveiliging en privacy beleid heeft de volgende doelen:

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

Het 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 betrokkenen wordt gerespecteerd en Albada voldoet aan relevante wet- en regelgeving, maar ook de bedrijfsvoering binnen Albada zo praktisch als mogelijk is binnen geldende kaders wordt ingericht.

3.2. Uitgangspunten

Albada is een open instelling waar veel mogelijk is. De benadering van ICT en beveiliging en privacy is minder open. Om de gestelde doelen van informatiebeveiliging en privacy te bereiken worden de volgende uitgangspunten gehanteerd:

1. Het College van Bestuur van Albada 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.
2. Albada voldoet aan de relevante wet- en regelgeving.
3. Bij Albada 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 Albada 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.
4. Albada informeert alle betrokkenen via bijvoorbeeld de privacy verklaring, 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.
5. Albada legt alle verwerkingen van persoonsgegevens vast in een dataregister en houdt deze up-to-date. Albada voldoet hiermee aan de documentatieplicht.
6. Binnen Albada 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. Albada is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert Albada informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en studenten worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. Albada 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, de benodigde investeringen en de te nemen maatregelen.
9. Albada sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van (een onderdeel van) Albada, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van

studenten of medewerkers worden verstrekt.

10. Albada verwacht van alle medewerkers, studenten, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Albada heeft een gedragscode geformuleerd, vastgesteld en geïmplementeerd (zie: [Gedragscode Gebruik Internet- Email- en \(mobiele\) Telefoonfaciliteiten.](#)). Met deze gedragscode moet worden voorkomen dat, door al dan niet opzettelijk gedrag, onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Bovendien wordt aan externen die met persoonsgegevens van Albada werken, gevraagd of zij een geheimhoudingsverklaring willen ondertekenen voordat zij toegang tot deze gegevens krijgen (kan ook verwerkt zijn in inhuurovereenkomsten e.d.).
11. Informatiebeveiliging en privacy is bij Albada een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. Albada 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. Albada 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. Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt Albada aanvullende afspraken vast over de technische maatregelen.
14. Albada zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en indien noodzakelijk melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

3.3. Reikwijdte

- Het IBP-beleid binnen Albada geldt voor alle medewerkers, studenten, ouders/verzorgers, (geregistreerde) bezoekers, externe relaties (inhuur / outsourcing), stagiaires en vrijwilligers. Onder dit beleid vallen ook alle devices (bijv. laptop, mobiele telefoon) van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Albada waaronder in ieder geval alle medewerkers, studenten, ouders/verzorgers, (geregistreerde) bezoekers, externe relaties (inhuur/outsourcing), stagiaires en vrijwilligers evenals op overige betrokkenen waarvan Albada persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen die vallen onder de verantwoordelijkheid van Albada. 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. (bijv. uitspraken van medewerkers en studenten 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 Albada, evenals voor 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 fysieke documenten zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- IBP-beleid heeft binnen Albada raakvlakken met:
 - a) **Algemeen veiligheids- en toegangsbeveiligingsbeleid**; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen,
 - b) **Personeels- en organisatiebeleid**; met als aandachtspunten in-, door- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties,
 - c) **IT-beleid**; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen, medezeggenschap van studenten, hun ouders/verzorgers en medewerkers.

4. Uitwerking

4.1. Informatie Beveiliging Plan (IBP)

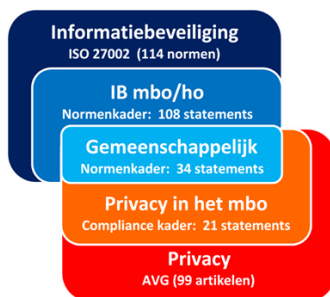
Om de informatiebeveiliging en privacy te verbeteren is er een plan waarin staat beschreven “wat” er moet gebeuren en “hoe” dit getoetst wordt, het zogenaamde informatiebeveiligingsplan.

4.2. Raamwerk “IBP in het MBO”

Albeda heeft er voor gekozen om niet zelf maatregelen te definiëren over wat er moet gebeuren, maar gebruikt het raamwerk “IBP in het MBO” dat is opgesteld door de regiegroep “IBP in het MBO” (Kennisnet, SURF en saMBO-ICT). Dit raamwerk wordt door een groot aantal MBO onderwijs instellingen gebruikt en is in overeenstemming met het doel, uitgangspunten en de reikwijdte van het IBP beleid.

4.3. Waar richten we ons op?

Normen beschrijven wat je zou kunnen doen, statements geven aan welke van de normen van toepassing zijn voor het Albeda. ISO 27002 beschrijft de normen op het gebied van informatiebeveiliging en de “Algemene verordening gegevensbescherming” (AVG) beschrijft wat organisaties moeten doen op het gebied van privacy. Voor beide geldt dat slechts een beperkte set van de normen van toepassing is op het MBO. Tussen de maatregelen om de informatiebeveiliging en de privacy te verbeteren is een overlap, deze overlap is in het raamwerk onderkend:



4.4. Uitwerking controle maatregelen

In het raamwerk staat wat er moet gebeuren. Hoe dit moet gebeuren moet verder worden uitgewerkt. Het verder uitwerken kan betekenen dat er iets moet gebeuren aan beleid, organisatie, procedures, werkbeschrijvingen en rapportage. Als het nodig is, met name op beleid en organisatie, zal de verdere uitwerking van de controlemaatregelen worden voorgelegd aan het CvB ter goedkeuring.

5. Organisatie – wie doet wat?

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

Niveau	Wie / Rollen	Verantwoordelijkheid / taken
Richtinggevend (strategisch)	CvB Directeur	<ul style="list-style-type: none"> 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
Richtinggevend (tactisch)	Regiegroep IBP	<ul style="list-style-type: none"> Geeft aan wat de risico's zijn vanuit verschillende perspectieven (onderwijs, juridisch, financieel, privacy en ICT) Bepaalt op basis van risico's de inhoud van het IBP plan Toetst specifieke IBP maatregelen De voorzitter rapporteert aan het CvB
Sturend (tactisch)	Manager informatiebeveiliging / CISO	<ul style="list-style-type: none"> 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
Uitvoerend (Operationeel)	FG	<ul style="list-style-type: none"> Toezicht op naleving privacy wetgeving Voorlichting privacy en stimuleren bewustwording Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens Afwikkeling klachten en incidenten
	ISO	<ul style="list-style-type: none"> Mede uitvoer geven aan het IBP plan Voorlichting over informatiebeveiliging en IBP beleid Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. informatiebeveiliging Risico analyse

Niveau	Wie / Rollen	Verantwoordelijkheid / taken
	Domeinverantwoordelijken / Proceseigenaren waaronder o.a.: ICT, HRM, Facilitair, Onderwijs, Financiën, Inkoop en Administratie	<ul style="list-style-type: none"> • Classificatie / risicoanalyse in samenwerking met CISO, ISO, FG • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/CvB/directie • 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.
	Functioneel en/of applicatie beheerder, medewerker	<ul style="list-style-type: none"> • Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures.
	Dagelijkse leiding / leidinggevende / directie	<ul style="list-style-type: none"> • 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 • periodiek het onderwerp informatiebeveiliging onder de aandacht brengen in werkoverleggen, beoordelingen etc. • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur
	Inkoop Juridisch	<ul style="list-style-type: none"> • Opstellen verwerking overeenkomsten • Afhandelen juridische aansprakelijkheid

6. Rapportage

Om goed te kunnen sturen op strategisch, tactisch en operationeel niveau is rapportage noodzakelijk. De rapportage op strategisch niveau is op basis van risico's en geeft aan welke doelstellingen er mogelijk een risico lopen door de mate van informatiebeveiliging. Deze rapportage moet minimaal twee keer per jaar plaatsvinden. De rapportage op tactisch niveau geeft aan wat de vorderingen zijn op de punten / normen vanuit het raamwerk en het IBP plan. Deze rapportage moet elke maand plaats vinden. Op operationeel niveau moet er management rapportage zijn over de operationele security processen, de frequentie van deze rapportage is één maal per week tot één maal per maand naargelang het proces.

7. Voorlichting en bewustzijn

Beleid, organisatorische en technische 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 en trainingen voor o.a. medewerkers, en studenten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de Chief Information Security Officer (CISO), de Functionaris Gegevensbescherming (FG), en de Information Security Officer (ISO) met het College van Bestuur CvB als eindverantwoordelijke.

8. 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, onderbreking van bedrijfsvoering processen en imagoverlies.

8.1. 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.*

8.2. Relevante wet- en regelgeving

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

- Wet Educatie Beroepsonderwijs (WEB)
- Branchecode 'Goed bestuur in het mbo'
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Naast bovengenoemde wet- en regelgeving zijn ook onderstaande aspecten van belang bij IBP:

- 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.

8.3. Basisregels voor het omgaan van persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 Algemene Verordening Gegevensbescherming (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 (Art 6 AVG), zie tevens [Autoriteit Persoonsgegevens](#)).

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 (hanteren wettelijke bewaartermijnen).
4. **Transparantie:** Albeda legt aan betrokkenen 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.

8.4. 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/of protocollen. Deze lijst wordt regelmatig aangepast aan de actualiteit. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

8.5. 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, zogenaamde BIV-classificatie.

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.

8.6. Incidenten en datalekken

Alle medewerkers en studenten 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 datalekken moeten worden gemeld bij de Functionaris Gegevensbescherming (FG) en (beveiligings-)incidenten bij de ICT Helpdesk. Periodiek worden de beveiligingsincidenten onderling besproken en waar nodig worden aanvullende beleidsmaatregelen genomen.

8.7. 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 Albeda 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 en overige van toepassing zijnde ontwikkelingen meegenomen.

8.8. 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 medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij bijv. de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode of met periodieke bewustwordingscampagnes.

Voor toezicht op de naleving van de AVG vervult de Functionaris 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 het bestuur vast te stellen reglement.

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

8.9. Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt er voor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens worden vastgelegd. Hieronder vallen o.a. het in- en uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk. Deze informatie wordt ook gebruikt voor het analyseren van datalekken en beveiligingsincidenten die zich hebben voorgedaan.