Samenwerkingsverband PO 3105
Passend Primair Onderwijs

Beleid Informatiebeveiliging en Privacy (IBP)

VASTGESTELD
DOOR HET BESTUUR OP
13.12.2021

PASSEND
PRIMAIR ONDERWIJS
MAASTRICHT EN HEUVELLAND

INHOUD

1. Het belang van informatiebeveiliging en privacy

Passend onderwijs werkt met uitwisselen van informatie, waaronder persoonsgegevens en ict. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ict en het werken met persoonsgegevens brengt nieuw 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 passend onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

De informatie en ict van het samenwerkingsverband worden blootgesteld aan een aantal bedreigingen, al dan niet opzettelijk van aard. Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's die gepaard gaan met deze bedreigingen tot een aanvaardbaar niveau te reduceren. Om dit structureel op te pakken is het noodzakelijk dat er duidelijk gemaakt wordt waar het om gaat, er een doel gesteld wordt en de manier aangegeven wordt waarop dit doel bereikt wordt.

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.

Dit wordt ook wel de BIV-classificatie genoemd.

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

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: *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 om informatiebeveiliging en privacy binnen het samenwerkingsverband te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3. Doel en reikwijdte

3.1 Doel

Informatiebeveiliging en privacy hebben de volgende doelen:

- Het waarborgen van de continuïteit van passend onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan het samenwerkingsverband persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers.
- 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 betrokkene (o.a. medewerker, leerling en hun ouder/verzorger) wordt gerespecteerd en het samenwerkingsverband voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

Het beleid kent de volgende reikwijdte:

- Het IBP-beleid binnen het samenwerkingsverband geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het netwerk van het samenwerkingsverband verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen het samenwerkingsverband waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan het samenwerkingsverband persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van het samenwerkingsverband. Hieronder valt tevens de gecontroleerde informatie, die door het samenwerkingsverband zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop het samenwerkingsverband kan worden aangesproken (bijv. uitspraken van medewerkers 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 het samenwerkingsverband evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- IBP-beleid heeft binnen het samenwerkingsverband raakvlakken met:
  - *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten 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) middelen
  - *Medezeggenschap*.

4. Beleid

Het samenwerkingsverband hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Informatiebeveiliging en privacy zijn een bestuursverantwoordelijkheid: dat betekent dat het bestuur de primaire verantwoordelijkheid draagt voor een goede informatiebeveiliging en privacy ten aanzien van (proces gebonden) informatie die binnen het samenwerkingsverband wordt gebruikt dan wel gegenereerd.
2. Binnen het samenwerkingsverband 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. Het samenwerkingsverband communiceert aan de medewerkers en verwerkers verwachtingen dat ze actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie.
3. Het samenwerkingsverband 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 afgedekt diene te worden en de benodigde investeringen en de te nemen maatregelen.
4. Het Samenwerkingsverband maakt met alle leveranciers van digitale middelen (bedrijfsapplicaties) concrete afspraken over informatiebeveiliging en privacy.
5. Informatiebeveiliging en privacy is bij het samenwerkingsverband een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
6. Bij projecten, zoals infrastructurele wijzigingen of de aanschaf van nieuwe systemen of het aanbieden van nieuwe services wordt vanaf de start rekening gehouden met informatiebeveiliging en privacy (Privacy by design).

5. Uitwerking en Uitvoering beleid

Praktische invulling van bovenstaande beleidspunten.

5.1 Relevante wet- en regelgeving

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

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet Passend Onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming
- 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.

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: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
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 staan tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiair). Dit betekent ook dat data niet langer worden bewaard dan noodzakelijk.
4. **Transparantie**: het samenwerkingsverband legt 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.

   Verder zijn er nog 4 ondersteunende regels:

6. Persoonsgegevens moeten adequaat worden **beveiligd** volgens algemeen en breed geaccepteerde beveiligingsnormen.
7. **Nieuwe verwerkingen** met bijzondere/gevoelige persoonsgegevens dienen vooraf ter goedkeuring aan het bestuur te worden voorgelegd met onderbouwing en privacy-afweging door de functionaris gegevensbescherming.
8. Verwerking van bestaande persoonsgegevens voor **nieuwe respectievelijk onderzoeks-doeleinden** zal eveneens vooraf ter goedkeuring aan het bestuur worden voorgelegd inclusief onderbouwing en privacy-afweging door de functionaris gegevensbescherming.
9. **Bijzondere persoonsgegevens** zijn als zodanig gelabeled en worden met aanvullende technische en organisatorische maatregelen beveiligd en getransporteerd (waaronder multi-factor authenticatie, logging en encryptie tijdens transport).

5.3 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. 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. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP en de FG, met het bestuur als eindverantwoordelijke. Dat gebeurt bij medewerkers in de aanstellingsbrief, tijdens functioneringsgesprekken, met organisatie brede gedragsregels, met periodieke bewustwordingscampagnes, etc.

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 (zie bijlage 3).

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.

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 kunnen worden gemeld bij de directie. 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 vier jaar - eventueel parallel aan het Ondersteuningsplan - 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 het samenwerkingsverband een jaarlijkse planning en control cyclus waarvan de informatiebeveiliging en privacy onderdeel uitmaakt. In bijlage 2 is het IBP toetsingskader met 22 statements opgenomen dat voor de evaluatie kan worden gebruikt.

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 de directie haar verantwoordelijkheid neemt en haar medewerkers aanspreekt in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met gedragsregels, etc. 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 op basis van een door het bestuur vast te stellen overeenkomst van opdracht.

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

5.9 Logging en monitoring

Logging en monitoring binnen de IT-omgeving 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.

6. Organisatie

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. Nader uitgewerkt in bijlage 1 - IBP rollen en taken.

IBP kent drie niveaus:

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

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

6.2 Richtinggevend - Eindverantwoordelijke

Het 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 directeur van het SWV.

6.3 Sturend -Directeur SWV

De directeur van het SWV is inhoudelijk verantwoordelijk voor IBP. De directeur geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau, waaronder:

- vertalen van het beleid naar richtlijnen, procedures, maatregelen, documenten en instructies
- bewaken uniformiteit binnen het samenwerkingsverband
- verlenen van autorisaties (toegang tot het netwerk en de netwerkdiensten waarvoor medewerkers specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben) en periodiek beoordelen toegangsrechten gebruikers
- periodiek het onderwerp IBP onder de aandacht brengen in werkoverleggen, personeelsgesprekken, etc.
- aanspreekpunt voor alle personeel gerelateerde IBP-onderwerpen
- aanspreekpunt voor incidenten op het gebied van informatiebeveiliging en privacy
- coördineren van de afhandeling van incidenten binnen het samenwerkingsverband.

6.4 Sturend - Functionaris voor Gegevensbescherming (FG)

De functionaris voor gegevensbescherming (FG) houdt binnen het samenwerkingsverband 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 directeur. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

6.5 Uitvoerend - Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven. Waar nodig worden deze medewerkers in hun dagelijkse werkzaamheden ondersteund.
Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid.
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere medewerker heeft op uitvoerend niveau de taak om op de hoogte zijn van het IBP-beleid en het IBP-beleid na te leven.

Bijlage 1: IBP rollen en taken

Niveau	Wie Rollen	Verantwoordelijkheid / taken	Documenten, o.a.
Richtinggevend (strategisch)	**Bestuur**	• Eindverantwoordelijk • IBP-beleidsvorming, vastleggen en uitdragen • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten • FG aanstellen	• Beleid Informatiebeveiliging en Privacy (IBP) • Privacyverklaring • Gedragsregels IBP • Overeenkomst van opdracht FG • Protocol beveiligingsincidenten en datalekken
Sturend (tactisch)	**Directeur**	• Inhoudelijk verantwoordelijk voor IBP • Implementeren IBP-maatregelen. • IBP-planning en controle • Adviseert bestuur over IBP • Voorbereiden uitvoeren IBP-beleid • (Laten) uitvoeren risicoanalyse • Hanteren IBP normen • Evalueren en actualiseren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen • Toegangsbeleid zowel fysiek als digitaal regelen • Autorisatie gebruikers en toegangsrechten gebruikers regelmatig beoordelen en controleren, incl. Wachtwoordbeleid • Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • 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. • Periodiek het onderwerp informatiebeveiliging onder de aandacht brengen in werkoverleggen, beoordelingen etc.; • Rapporteren realisatie doelstellingen IBP-beleid aan bestuur. • Security awareness activiteiten	• Verwerkersovereenkomsten • Autorisatiematrix • Informatiedocumentatie voor betrokkenen • Dataregister • Risicoanalyse • DPIA (indien van toepassing)
	FG	• 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	
Uitvoerend (operationeel)	**Mede-werker**	• Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	

Bijlage 2: Toetsingskader IBP

	IBP statement
P.01	Privacy beleid, uitgangspunten en toewijzing taken/verantwoordelijkheden
P.02	Functionaris gegevensbescherming
P.03	Naleving uitgangspunten privacy in uitvoeringsdomein
P.04	Registratieplicht
P.05	Bewaartermijnen
P.06	Verwerking t.b.v. onderzoek
P.07	Beleid bijzondere persoonsgegevens
P.08	Geautomatiseerde besluitvorming
P.09	Informatiebeveiliging
P.10	Bewerkersovereenkomsten
P.11	Transparantie privacy beleid
P.12	Informatieplicht verwerkingen
P.13	Rechten van betrokkene
P.14	Arbeidsvoorwaarden
P.15	Bewustzijn, opleiding en training ten aanzien van privacy
P.16	Verwijderen van persoonsgegevens
P.17	Datakwaliteit (data-integriteit)
P.18	Meldplicht datalekke inclusief registratie
P.19	Bijzondere persoonsgegevens (extra maatregelen)
P.20	Privacy in informatiesystemen
P.21	Gegevensbeschermingseffectbeoordeling (GEB / PIA)
P.22	Naleving van privacybeleid en –normen

Bijlage 3: Gehanteerde classificatie standaard

Bij het samenwerkingsverband zijn alle gegevens waarop dit informatiebeveiligingsbeleid van toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses.
Daarbij zijn de volgende kwaliteitsaspecten van informatievoorziening van belang:

Beschikbaarheid: De mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ICT-dienstverlening waarborgen.

Integriteit: De mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.

Vertrouwelijkheid: De mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.

A. Beschikbaarheid

Ten aanzien van de beschikbaarheidseisen is voor de volgende classificatie gekozen:

Classificatie indeling	Classificatie gevolg	Beheersmaatregel
Beschikbaarheid **Laag**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende **langer dan 1 week** brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers, stagiaires, vrijwilligers of cliënten/klanten.	Wekelijkse back-up
Beschikbaarheid **Midden**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende **langer dan 48 uur** brengt merkbare schade toe aan de belangen van de organisatie, haar medewerkers, stagiaires, vrijwilligers of cliënten/klanten.	Dagelijkse back-up
Beschikbaarheid **Hoog**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende **langer dan 1 uur** brengt merkbare schade toe aan de belangen van deinstelling, haar medewerkers, stagiaires, vrijwilligers of cliënten/klanten.	Synchronisatie met externe locatie

B. Integriteit

Voor integriteit wordt de volgende classificatie indeling gehanteerd:

Classificatie indeling	Classificatie gevolg	Beheersmaatregel
Integriteit **Laag**	Het bedrijfsproces staat **enkele** integriteitsfouten toe.	Applicatie controle
Integriteit **Midden**	Het bedrijfsproces staat **zeer weinig** integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk.	Applicatie plus menselijke controle
Integriteit **Hoog**	Het bedrijfsproces staat **geen** integriteitsfouten toe.	Applicatie plus twee maal menselijke controle

C. Vertrouwelijkheid

Vertrouwelijkheid is als volgt geclassificeerd:

Classificatie indeling	Classificatie gevolg	Beheersmaatregel
Vertrouwelijkheid **Laag**	Informatie die toegankelijk mag of moet zijn voor **alle of grote groepen** medewerkers, stagiaires, vrijwilligers of cliënten/klanten. Vertrouwelijkheid is gering.	Toegang tot netwerk op basis van arbeidsovereenkomst of inschrijving.
Vertrouwelijkheid **Midden**l	Informatie die alleen toegankelijk mag zijn voor een **beperkte groep** gebruikers. De informatie is vertrouwelijk.	Toegang op basis van autorisatiematrix.
Vertrouwelijkheid **Hoog**	Dit betreft zeer vertrouwelijke informatie, alleen bedoeld voor **specifiek benoemde personen**, waarbij onbedoeld bekend worden buiten deze groep grote schade kan toe brengen.	Toegang op basis van Autorisatiematrix plus pasje of sms code (multifactor authentication)

Welk beveiligingsniveau geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt. De classificatie dient door de proceseigenaar te worden bepaald.

Voorbeeld classificatie en labelen

Deze classificatie wordt samengevat tot BIV (Beschikbaarheid-Integriteit-Vertrouwelijkheid) waar vervolgens door de proceseigenaren scores aan worden toegevoegd. Zo zou de proceseigenaar HR het HR-dossier kunnen classificeren met Integriteit en Vertrouwelijkheid Hoog. Kort weergegeven als BIV M-H-H. Het gelabelde proces verzuimdossier wordt geclassificeerd M-H-H.