INFORMATIEVEILIGHEIDS- EN PRIVACYBELEID

vzw Diocesaan Schoolcomité Sint-Niklaas

Collegestraat 31

9100 SINT-NIKLAAS

voor:

Internaat Sint-Jozef-Klein-Seminarie

Collegestraat 31

9100 SINT-NIKLAAS

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-08-24	GELDIG	Internaat SJKS	

Inhoud

1 Inleiding

Informatie en ICT zijn noodzakelijk voor de administratie en begeleiding. Denken we maar aan de (intern)administratie- en (intern)volgsystemen. Vaak verwerken deze geautomatiseerde systemen persoonsgegevens (van internen, ouders, personeelsleden…) en is de privacywetgeving (GDPR of AVG) hierop van toepassing.

Deze informatieverwerking en het gebruik van ICT brengen risico's met zich mee. Denken we bijvoorbeeld maar aan een cyberaanval waarbij de gegevens versleuteld worden, een vergissing waardoor gegevens onherroepelijk gewist zijn, de natuur (bijv. overstroming of brand), et cetera. Het niet beschikbaar zijn van ICT, incorrecte administraties en het uitlekken van gegevens kan leiden tot inbreuken.

Deze bedreigingen maken het noodzakelijk om adequate maatregelen te nemen op het gebied van informatieveiligheid en privacy (IVP) 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 we een duidelijk maken waar het om gaat, een doel stellen en de manier waarop we dit doel willen bereiken.

1.1 Toelichting informatieveiligheid

Onder informatieveiligheid wordt verstaan: het nemen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatie en ICT zo maximaal mogelijk te garanderen.

Deze kwaliteitsaspecten zijn:

- **Beschikbaarheid:** de mate waarin persoonsgegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- **Integriteit:** de mate waarin gegevens en/of functionaliteiten juist, volledig en actueel zijn.
- **Vertrouwelijkheid:** de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.
- **Controleerbaarheid:** de mate waarin het mogelijk is om achteraf parameters die van belang zijn voor beschikbaarheid, integriteit of vertrouwelijkheid te verifiëren.

Onvoldoende informatieveiligheid kan leiden tot onacceptabele risico's bij de dagdagelijkse werking van de organisatie. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagoverlies.

1.2 Toelichting privacy

Privacy gaat over de verwerking van persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform de huidige wet- en regelgeving. De bescherming van de privacy regelt onder andere de voorwaarden waaronder persoonsgegevens gebruikt mogen worden.

Persoonsgegevens zijn hierbij alle gegevens van een geïdentificeerd of identificeerbaar individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. Denken we maar aan het verzamelen, raadplegen, bijwerken, verspreiden tot met het wissen van deze gegevens.

1.3 Vervlechting informatieveiligheid en privacy

Informatieveiligheid is noodzakelijk om privacy te waarborgen. Beide begrippen zijn met elkaar verbonden. Het onderwerp informatieveiligheid en privacy wordt afgekort tot IVP. Deze beleidstekst ligt ten grondslag aan de aanpak van informatieveiligheid en privacy binnen Internaat Sint-Jozef-Klein-Seminarie.

2 Doel en reikwijdte

2.1 Doel

Dit beleid heeft als doelen:

- Het waarborgen van de continuïteit en de dagdagelijkse werking van Internaat Sint-Jozef-Klein-Seminarie.
- Het garanderen van de privacy van internen, ouders, personeelsleden, derden,… waardoor beveiligings- en privacy-incidenten zoveel mogelijk worden voorkomen.

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een goede balans moet zijn tussen privacy, functionaliteit, veiligheid en middelen. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van personeelsleden, internen en ouders wordt gerespecteerd en dat Internaat Sint-Jozef-Klein-Seminarie voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Internaat Sint-Jozef-Klein-Seminarie waaronder in ieder geval: alle personeelsleden, internen, ouders/voogden, (geregistreerde) bezoekers en externe relaties, evenals op andere betrokkenen waarvan Internaat Sint-Jozef-Klein-Seminarie persoonsgegevens verwerkt.
- Dit beleid is van toepassing op zowel de digitale als geschreven verwerking van persoonsgegevens.
- Het IVP-beleid geldt voor alle personeelsleden, internen, ouders/voogden, (geregistreerde) bezoekers en externe relaties die uit hoofde van hun taak, op het internaat of thuis persoonsgegevens verwerken.
- Het beleid heeft betrekking op gecontroleerde informatie die door onszelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de instelling kan worden aangesproken, zoals uitspraken van personeelsleden en internen in discussies, op (persoonlijke pagina's van) websites en sociale media. Hiervoor werkt Internaat Sint-Jozef-Klein-Seminarie met **gedragscodes**.
- Het IVP-beleid binnen Internaat Sint-Jozef-Klein-Seminarie heeft 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 personeelsleden, functiewisselingen, functiescheiding en vertrouwensfuncties;
  - IT-beleid; met als aandachtspunten de aanschaf, het beheer, het gebruik en/of het uit dienst stellen van hardware, software en services;
  - Participatie van internen, hun ouders/voogden en personeelsleden.

3 Uitgangspunten

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Internaat Sint-Jozef-Klein-Seminarie zijn:

- IVP dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de **Algemene Verordening Gegevensbescherming** (AVG).
  De verwerking van persoonsgegevens is steeds gebaseerd op één van de in deze verordening vastgelegde rechtmatigheden. Hierbij willen we een goede balans zoeken tussen het belang van Internaat Sint-Jozef-Klein-Seminarie om persoonsgegevens te verwerken en het belang van de betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn/haar persoonsgegevens.

- Het schoolbestuur/internaatsbestuur, vzw Diocesaan Schoolcomité Sint-Niklaas, is als rechtspersoon de **verwerkingsverantwoordelijke** voor alle persoonsgegevens die in opdracht van Internaat Sint-Jozef-Klein-Seminarie verwerkt worden.

- Internaat Sint-Jozef-Klein-Seminarie sluit met alle **verwerkers** een **verwerkersovereenkomsten** af indien deze persoonsgegevens ontvangen van de instelling.

- Binnen Internaat Sint-Jozef-Klein-Seminarie 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 fysieke documenten.

- Er wordt van alle personeelsleden, internen, (geregistreerde) bezoekers en externe relaties verwacht 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 imagoverlies. In het *algemeen reglement van het personeel van het katholiek onderwijs* (artikel 7 § 7) wordt hiernaar verwezen.

- Bij wijzigingen in de infrastructuur, de aanschaf en de uit dienst name van (informatie)systemen, wordt bij Internaat Sint-Jozef-Klein-Seminarie steeds rekening gehouden met IVP.

- IVP is bij Internaat Sint-Jozef-Klein-Seminarie een continu proces, waarbij regelmatig (minimaal 1x per jaar) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

3.2 Uitgangspunten privacy

De zes vuistregels met betrekking tot de omgang van persoonsgegevens bij Internaat Sint-Jozef-Klein-Seminarie zijn:

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 verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op één van de wettelijke rechtmatigheden: toestemming, overeenkomst, wettelijke verplichting, openbaar belang, 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 tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt.
4. **Transparantie**: de instelling legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IVP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op inzage, verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Opslagbeperking:** data wordt niet langer bewaard dan noodzakelijk. De verwerking wordt door het IVP-beleid beperkt in de tijd.
6. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn, en dat zij voldoende beschikbaar zijn om de werking van Internaat Sint-Jozef-Klein-Seminarie te waarborgen. Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van **toestemming**, zal Internaat Sint-Jozef-Klein-Seminarie een eenduidige procedure hanteren die een actieve en aantoonbare handeling vereist.

4 Wet- en regelgeving

Internaat Sint-Jozef-Klein-Seminarie voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Algemene Verordening Gegevensbescherming (AVG)
- Camerawet
- Auteurswet

5 Organisatie

De organisatie van IVP gaat over procedures, afspraken en regels die van betekenis zijn voor de manier waarop mensen een organisatie besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Dit hoofdstuk beschrijft hoe IVP in Internaat Sint-Jozef-Klein-Seminarie is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

Voor elk niveau wordt beschreven welke verantwoordelijkheden en taken de verschillende rollen met zich meebrengen.

5.1 Rollen (functies) rondom IVP

Om IVP gestructureerd en gecoördineerd aan te pakken worden bij Internaat Sint-Jozef-Klein-Seminarie een aantal rollen aan personeelsleden in de bestaande organisatie toegewezen.

5.2 Richtinggevend

Verwerkingsverantwoordelijke

Het schoolbestuur of internaatsbestuur is eindverantwoordelijk voor IVP en stelt het beleid en de basismaatregelen op het gebied van IVP vast.

De toepassing en werking van het IVP-beleid wordt op basis van regelmatige rapportages geëvalueerd.

Zie bijlage 1 voor een schematische weergave van de rol- en taakverdelingen aangaande IVP op Internaat Sint-Jozef-Klein-Seminarie en binnen vzw Diocesaan Schoolcomité Sint-Niklaas.

5.3 Sturend

Data Protection Officer (DPO) van de koepelorganisatie

Vanuit de koepelorganisatie Katholiek Onderwijs Vlaanderen wordt er een Data Protection Officer aangesteld. Deze zal binnen het schoolbestuur of instelling het Aanspreekpunt Informatieveiligheid (AIV) aansturen. De taak bestaat uit:

- besturen informeren en adviseren over hun verplichtingen vanuit de AVG en vanuit andere gegevensbeschermingsbepalingen;
- AIV's opleiden en hulpmiddelen verstrekken zodanig dat ze binnen hun instelling(en) het IVP-beleid kunnen ondersteunen;
- desgevraagd advies verstrekken over de gegevensbeschermingseffectbeoordeling;
- met de toezichthoudende autoriteit samenwerken en optreden als aanspreekpunt voor deze autoriteit.

Aanspreekpunt Informatieveiligheid

Het AIV is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (directie/beheerder van de instelling, raad van bestuur van het schoolbestuur/internaatsbestuur) en staat de mensen op uitvoerend niveau bij. Het AIV moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen Internaat Sint-Jozef-Klein-Seminarie
- Meewerken aan de bewustmaking en opleiding van het personeel
- Het aanspreekpunt zijn voor incidenten op het gebied van IVP
- De verdere afhandeling van incidenten binnen Internaat Sint-Jozef-Klein-Seminarie coördineren

5.4 Uitvoerend

Leidinggevende

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

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

De leidinggevende kan in zijn taak ondersteund worden door het AIV.

ICT-coördinator

De ICT-coördinator vormt een technisch aanspreekpunt inzake informatieveiligheid voor het management en de personeelsleden, en zorgt in de praktijk voor de implementatie van toegangsrechten en de rapportage aangaande

Personeelsleden

Alle personeelsleden hebben een verantwoordelijkheid met betrekking tot informatieveiligheid in hun dagelijkse werkzaamheden. Daarnaast worden personeelsleden in hun dagelijkse werkzaamheden, waar nodig, ondersteund.

Personeelsleden wordt gevraagd om actief betrokken te zijn bij informatieveiligheid. Dit kan door meldingen te maken van beveiligingsincidenten, het doen van voorstellen ter verbetering van IVP en het uitoefenen van invloed op het beleid (individueel of via de ervoor voorziene overlegorganen en/of via het aanspreekpunt). Zelf hebben zij ook een voorbeeldfunctie naar andere personeelsleden, externen en internen toe.

Van ambtswege uit, of eventueel contractueel, worden alle medewerkers (ook extern) van Internaat Sint-Jozef-Klein-Seminarie die toegang kunnen hebben tot persoonsgegevens, gebonden aan een discretieplicht.

6 Controle en rapportage

Dit IVP-beleid en alle bijhorende richtlijnen, nota's en tools, worden minimaal elke twee jaar getoetst en bijgesteld door het schoolbestuur. Hierbij wordt rekening gehouden met:

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

Daarnaast kent Internaat Sint-Jozef-Klein-Seminarie een jaarlijkse planning en controlecyclus voor IVP. Dit is een vast evaluatieproces waarmee de inhoud en effectiviteit van het IVP-beleid wordt getoetst.

Voor alle overlegmomenten geldt dat deze **zoveel mogelijk ingepast worden in bestaande overlegvormen** met hetzelfde karakter waarbij op:

- **strategisch** niveau (richtinggevend) wordt gesproken over organisatie, alsmede over doelen, bereik en ambitie op het gebied van IVP.
- **tactisch** niveau (sturend) de strategie wordt vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.
- **operationeel** niveau (uitvoerend) de onderwerpen worden besproken die de dagelijkse uitvoering aangaan. Deze overlegvorm wordt niet centraal georganiseerd, en indien nodig in elk organisatieonderdeel van Internaat Sint-Jozef-Klein-Seminarie afzonderlijk.

6.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatieveiligheid en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij Internaat Sint-Jozef-Klein-Seminarie 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 onder andere de regelmatig terugkerende bewustwordingscampagnes voor iedereen binnen de instelling. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van het AIV en leidinggevende(n), met de raad van bestuur van vzw Diocesaan Schoolcomité Sint-Niklaas als eindverantwoordelijke.

6.2 Classificatie en risicoanalyse

Bij Internaat Sint-Jozef-Klein-Seminarie heeft alle informatie waarde. Er kan gebruik worden gemaakt van een systeem, om alle persoonsgegevens waarop dit beleid van toepassing is, te classificeren. De risicoanalyse zal het niveau van de beveiligingsmaatregelen bepalen rekening houdend met de classificatie van de gegevens. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang zijn voor de informatievoorziening.

6.3 Incidenten en gegevenslekken

Bij Internaat Sint-Jozef-Klein-Seminarie is het melden van beveiligingsincidenten en gegevenslekken vastgelegd in een protocol.

Alle incidenten kunnen worden gemeld bij privacy@sjks.be. De afhandeling van deze incidenten volgt een gestructureerd proces, waarbij men ook voorziet in de juiste stappen rondom de meldplicht gegevenslekken.

6.4 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IVP proces. Van belang hierbij is dat leidinggevenden hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij Internaat Sint-Jozef-Klein-Seminarie wordt actief aandacht besteed aan IVP bij de aanstelling, tijdens functioneringsgesprekken, met een gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Mocht de naleving ernstig tekort schieten, dan kan Internaat Sint-Jozef-Klein-Seminarie de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden. Voor de bevordering van de naleving van de AVG heeft het AIV een belangrijke rol.

Bijlage 1: Tabel IVP rollen en taken

Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
Schoolbestuur of internaatsbestuur	• Eindverantwoordelijke • IVP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IVP-beleid op basis van rapportages en bijsturen van dit beleid indien nodig • Organisatie IVP inrichten	• Informatieveiligheids- en privacy beleid opstellen en goedkeuren en communiceren • Aanspreekpunt informatieveiligheid aanstellen • Oprichten veiligheidscel
Leidinggevende (directie, beheerder)	• Toezien op de naleving van het IVP-beleid en privacywetgeving en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Communicatie naar alle betrokkenen; er voor zorgen dat alle medewerkers op de hoogte zijn van het IVP-beleid en de consequenties ervan. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IVP-beleid. • Rapporteren voortgang m.b.t. doelstellingen IVP-beleid aan bestuur • Periodiek het onderwerp informatiebeveiliging onder de aandacht brengen in werkoverleg, beoordelingen,… • Implementeren IVP-maatregelen.	Communiceren, informeren en toezien op naleving van o.a.: • IVP in het algemeen • Hoe omgaan met leerlingendossiers • Wie mag wat zien • Gedragscode • Beveiliging van ruimtes • Preventieve maatregelen (o.a. brand en waterschade aan servers…) • …
Data protection officer koepel	• Schoolbesturen/internaatsbesturen informeren en adviseren over hun verplichtingen krachtens de AVG en regelgeving; • Richtlijnen, kaders, procedures opstellen en aanbevelingen doen m.b.t. informatieveiligheid en privacy • Aanspreekpunten IVP opleiden en hen de nodige tools en hulpmiddelen verstrekken • desgevraagd advies verstrekken over de gegevensbeschermingseffectbeoordeling • samenwerken met de toezichthoudende autoriteit en optreden als aanspreekpunt voor deze autoriteit • Brugfiguur naar de externe partijen toe • Lerend netwerk ontwikkelen en aansturen	• Opstellen van algemene processen, richtlijnen en sjablonen IVP • Nascholingstraject organiseren • Overleg met informatieveiligheidsconsulenten onderwijsnetten en GO! • Overleg met externe partijen: leveranciers van leerlingadministratie en -volgsysytemen en leveranciers van didactische software • Tools aanpassen/ontwikkelen

Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**

Aanspreekpunt informatieveiligheid	• Informeert en adviseert directie/beheerder/bestuur en personeel over IVP
	• Rapporteert naar directie/beheerder/bestuur
	• Informeert de data protection officer van de koepel
	• Meewerken aan de uitwerking van een specifiek IVP-beleid op basis van het algemeen IVP-beleid
	• Voorstellen doen tot aanpassingen van centraal aangeboden processen, richtlijnen en procedures om de uitvoering van het IVP-beleid te ondersteunen binnen de instelling
	• Meewerken aan:
	  ○ classificatie van middelen
	  ○ risicoanalyse
	  ○ het opstellen van een veiligheidsplan
	• Aanspreekpunt voor IVP-incidenten
	• Incidentafhandeling (registreren en evalueren).
	• Invullen register verwerkingsactiviteiten
		Voorstellen van aanpassingen aan de uitgewerkte formulieren van processen, richtlijnen en procedures rond IVP, bijvoorbeeld:
		
		• Security awareness activiteiten
		• Authenticatie en autorisatie-beleid
		• Gedragscodes (ICT en internetgebruik, sociale media, privacybeleid…) naar medewerkers en leerlingen toe
		• Verwerkersovereenkomsten regelen
		• Toestemming opstellen gebruik foto's en video
		• Communicatieplan naar medewerkers, leerlingen, ouders en cursisten
		• Procedure IVP-incident afhandeling
		• Inrichten meldpunt datalekken
		• Melden datalekken naar de overheid toe
		• …
		Invullen van register verwerkingsactiviteiten voor de eigen situatie

Informatieveiligheids cel (CIV) van de school/internaat of het schoolbestuur [1]	• Classificatie van informatie • IVP risicoanalyse uitvoeren • Prioriteiten voorstellen • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten bekrachtigen door bestuur • De toegangsrechten van gebruikers regelmatig beoordelen en controleren. • Evalueren IVP-beleid en voorstellen van verbetermaatregelen • Bespreking veiligheidsincidenten en voorstellen formuleren voor te nemen maatregelen • Aanpassen gegevensbeschermings-effectbeoordeling aan eigen situatie	• Inventariseren waar persoonsgegevens van de organisatie terechtkomen (leveranciers lijst) • Classificatie van informatiebronnen en persoonsgegevens • Risicoanalyse uitvoeren en documenteren Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk
Iedereen	• Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IVP bij de dagelijkse werkzaamheden	Richtlijnen en procedures volgen Melden incidenten aan aanspreekpunt informatieveiligheid

[1] bestaande uit domeinverantwoordelijke/ proceseigenaren waaronder: ICT, personeelsdienst, preventieadviseur, financiën, leerlingenadministratie, facilitair management, leidinggevende en het aanspreekpunt informatieveiligheid

Bijlage 2: Aanvullende nota's

Bij dit algemene deel van het IVP-beleid horen nog enkele specifieke nota's :

- Gebruikersrechtenbeleid
- Wachtwoordbeleid
- Communicatiebeleid
- Toestelbeleid
- Backupbeleid