# *informatiebeveiliging- en privacy beleid*

*Samen* **ict** *voor onderwijs*

**Coöperatie KIEN U.A.**

**Laan der Verenigde naties 325**
**3318 LA  Dordrecht**

**Postbus 1184**
**3300 BD  Dordrecht**

**T 088 657 5000**
**info@KIENict.nl**
**www.KIENict.nl**

**KVK 55645704**

## Verantwoording

**Bron:**
saMBO-ICT
Kennisnet

**Bewerkt door:**
KIEN U.A. , I. Meere

| Versie | Status | Datum | Auteur | Omschrijving |
|---|---|---|---|---|
| 0.1 | draft | 16-9-2016 | I.Meere | Eerste uitwerking template Kennisnet |
| 1.0 | definiteif | 22-11-2017 | I.Meere | Accordering van 0.1 en opgenomen in de product diensten catalogus |
| 1.0 | definitief | 8-2-2018 | G. Reijnders | IBP beleid als hoodstuk opgenomen in PDC |

# 1 Inleiding

Het onderwijsveld is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. KIEN neemt een deel van deze verantwoordelijkheden over en een deel blijft bij de onderwijs instellingen. Belangrijk is dat er een goed overzicht is wat bij KIEN ligt en waar de leden zelf voor verantwoordelijk zijn. De afhankelijkheid van elkaar en het toegenomen belang van informatie beveiliging brengt nieuwe kwetsbaarheden en risico's met zich mee. Het is van belang om een goede afstemming en adequate maatregelen te nemen om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering van KIEN en haar leden optimaal te kunnen waarborgen.

Dit document is een richting gevend document. Nog niet alles in dit beleidsstuk is al in werking bij schrijven. In mei 2018 zal Kien aan het gestelde beleid voldoen. Dan zal dit document worden opgenomen in de PDC

## 1.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen.
Deze aspecten zijn:

- 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 onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van KIEN en haar leden. Incidenten en inbreuken in deze processen kunnen leiden tot imagoverlies en financiële schade voor KIEN en daarbij al haar leden.

## 1.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform huidige wet – en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. 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.

## 1.3 Vervlechting informatiebeveiliging en privacy (IBP)

Uit voorgaande blijkt dat privacy een integraal onderdeel is van informatiebeveiliging.
Informatiebeveiliging en privacy (IBP) zal bij KIEN U.A. worden vastgelegd in dit beleidsplan, dat ten grondslag ligt aan de aanpak van informatiebeveiliging en privacy binnen KIEN. Hiernaast moeten de leden hun eigen IBP hebben, deze plannen zullen een sterke verwevenheid hebben. De wens is om een gezamenlijke FG aan te stellen met alle leden.

# 2 Doel en reikwijdte

## 2.1 Doel

***Het informatiebeveiliging- en privacy beleid (IBP) bij KIEN U.A. heeft als doelen:***

- ***Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering van alle leden beperkt tot het gebied van de dienstverlening van KIEN U.A..***
- ***Het minimaliseren van schade en de eventuele gevolgen hiervan door het voorkomen van beveiligings- en privacy-incidenten.***

Het beleid van KIEN U.A. is er op gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet zijn tussen privacy, functionaliteit en veiligheid. Uitgangspunt is dat persoonlijke levenssfeer van de betrokkene, medewerkers en leerlingen, wordt gerespecteerd en voldoet aan relevante wet- en regelgeving.

## 2.2 Reikwijdte

- Het informatiebeveiligings- en het privacy beleid binnen KIEN U.A. heeft betrekking op alle medewerkers, gebruikers en externe relaties (inhuur / outsourcing), alsmede op alle organisatieonderdelen. Tevens vallen onder dit beleid alle devices van waar geautoriseerde toegang tot het netwerk van KIEN of haar leden verkregen kan worden.

- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van KIEN U.A.. Het beleid heeft zowel betrekking op gecontroleerde informatie, die door de KIEN zelf is gegenereerd en wordt beheerd, als ook op niet-gecontroleerde informatie, waaronder uitspraken van medewerkers in discussies, persoonlijke websites op zakelijke personal pages, waarop KIEN kan worden aangesproken. Belangrijk is dat de informatie die geproduceerd wordt door de leden van KIEN buiten de verantwoordelijkheid van KIEN valt.

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen KIEN U.A. waaronder in ieder geval de persoonsgebonden gegevens van alle data die kien beheert, van haarzelf en van haar leden.

- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van KIEN U.A. evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Eveneens is het beleid 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 binnen KIEN U.A. heeft raakvlakken met:
  - Personeels- en organisatie beleid
  - IT-beleid zowel intern als van de leden
  - Algemeen veiligheids- en toegangsbeveiligingsbeleid
  - Bedrijfscontinuïteit

# 3 Uitgangspunten

## 3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij KIEN U.A. zijn:

Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming (die 25 mei 2018 in werking treedt).
De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van KIEN U.A. om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.

- Binnen KIEN U.A. is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie.

- KIEN U.A. is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert KIEN informatie van haar leden, waarvan het eigendom toebehoort aan het lid.

- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij KIEN U.A. geclassificeerd. De classificatie is het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse, waarbij gebruik gemaakt wordt van de classificatie. Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen → per januari 2018

- Bij KIEN U.A. wordt met alle leveranciers van digitale middelen, voor zover noodzakelijk, bewerkersovereenkomsten afgesloten.

- Er wordt van alle medewerkers, gasten, 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. Het is om deze reden dat er bij KIEN U.A. gedragscodes zijn geformuleerd, vastgesteld en geïmplementeerd.

- Informatiebeveiliging en privacy is bij KIEN U.A. een continu proces, waarbij regelmatig gekeken zal worden of aanpassing nodig is.

- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij KIEN U.A. vanaf de start rekening gehouden met informatiebeveiliging en privacy, dit is een taak van de proceseigenaren

## 3.2 Beleidsuitgangspunten privacy

De specifieke beleidsuitgangspunten met betrekking tot privacy bij KIEN U.A. zijn:

- Verwerking van Persoonsgegevens is gebaseerd op een van de meest relevante wettelijke grondslagen

- Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd.
- Bij de verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de Persoonsgegevens die strikt noodzakelijk zijn voor het specifieke doel. De gegevens moeten met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn.
- Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en moet in redelijke verhouding te staan tot het beoogde doel.
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen.
- Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
- Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen.
- Iedere Betrokkene heeft recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van de in de afzonderlijke verwerkingen hem betreffende Persoonsgegevens, en heeft het recht van verzet.
- De school kan aan betrokkenen op transparante wijze verantwoording afleggen over de verwerkingen en de daarbij gehanteerde principes.
- Bij alle registraties op vrijwillige basis zal aan de Betrokkene na toestemming een eenduidige zogenaamde Opt-out procedure worden aangeboden.

# 4 Wet- en regelgeving

Bij KIEN U.A. voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

# 5 Organisatie

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.
Dit hoofdstuk beschrijft hoe IBP bij KIEN U.A. is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

Voor elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen

## 5.1 Richtinggevend

**Eindverantwoordelijke**

De Almenene Ledenvergadering en directie KIEN U.A. zijn 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 manager IBP.

## 5.2 Sturend

**Manager IBP**

Manager IBP wordt als rol sturend niveau belegd bij de operational manager. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op uitvoerend niveau. De manager IBP moet:

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

**Functionaris voor Gegevensbescherming (nog aan te stellen Operational Manager ad intrim)**

De functionaris voor gegevensbescherming (FG) houdt binnen KIEN U.A. 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 afhandelen van vertrouwelijke informatiebeveiligingsincidenten. De FG is ook de contactpersoon en voor klachten en vragen van betrokkenen.

**Productblad eigenaar / proceseigenaar**

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

De productblad eigenaar / 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 het directeur stellen zij het beleid voor toegang vast.
- Samen met functioneel beheer en ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
- Samen met functioneel beheer en ICT-beheer beoordelen zij regelmatig de toegangsrechten van gebruikers.

## 5.3 Uitvoerend

**Security Officer (nog aan te stellen)**

De Security Officer vormt een technisch aanspreekpunt inzake informatiebeveiliging voor het management en de medewerkers.

**Medewerker**
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in 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 andere 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.

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

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;
- 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.

# 6 Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt jaarlijks getoetst en bijgesteld door het MT. Hierbij wordt rekening gehouden met:

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

## 6.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij KIEN U.A. 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, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de manager IBP met de directie als eindverantwoordelijke.

## 6.2 Classificatie en risicoanalyse (vanaf januari 2018)

Bij KIEN U.A. heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt be-

paald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang voor de informatievoorziening.

### 6.3 Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij helpdesk@kienict.nl. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

### 6.4 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevenden en productbladeigenaren/proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij KIEN U.A. wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de Algemene Ledenvergadering, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door de Algemene Ledenvergadering nog vast te stellen regelement. Mocht de naleving ernstig tekort schieten, dan kan KIEN U.A.de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.
Bij KIEN U.A. is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

| Niveau | Wie<br>Rollen | Hoe<br>Verantwoordelijkheid / taken | Wat<br>Realiseren / vastleggen |
|---|---|---|---|
| **Richtinggevend (strategisch)** | ALV<br>Directeur | • Eindverantwoordelijk<br>• IBP-beleidsvorming, -vastlegging en het uitdragen ervan<br>• Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens<br>• Evalueren toepassing en werking IBP-beleid op basis van rapportages<br>• Organisatie IBP inrichten | • Informatiebeveiligings- en privacy beleid<br>• Reglement FG |
| **Sturend (tactisch)** | Operational Manager met als aanvullende rol Manager IBP | • Inhoudelijk verantwoordelijk voor IBP<br>• IBP-planning en controle<br>• Adviseert directie over IBP<br>• Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse<br>• Hanteren IBP normen en wijze van toetsen<br>• Evalueren IBP-beleid en maatregelen<br>• Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze<br>• Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen | Risicoanalyse<br><br>IBP processen, (basis)richtlijnen en procedures informatiebeveiliging en privacy |
| | FG | • Toezicht op naleving privacy wetgeving<br>• Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens<br>• Afwikkeling klachten en incidenten | • Privacyreglement, |
| | Productblad eigenaar & FB interne applicaties | • **Classificatie / risicoanalyse** *in samenwerking met Operationeel Manager*<br><br>• Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door *directie*<br><br>• *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.<br><br>• *Samen met functioneel beheer en ICT* beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren. | Classificatie- en risicoanalyse documenten.<br><br>Diverse beleidsstukken, richtlijnen, procedures en protocollen<br><br>Aanvullende specifieke beleidsstukken |

| Niveau | Wie<br>Rollen | Hoe<br>Verantwoordelijkheid / taken | Wat<br>Realiseren / vastleggen |
|---|---|---|---|
| **Uitvoerend (operationeel)** | Productblad eigenaar | • Incidentafhandeling (registreren en evalueren)<br>• Technisch aanspreekpunt voor IBP-incidenten | • procedure IBP-incident afhandeling<br>• Inrichten meldpunt datalekken |
| | Medewerker | • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden | |
| | Dagelijkse leiding | • Communicatie alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan<br>• Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers.<br>• Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid<br>• Implementeren IBP-maatregelen<br>• periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;<br>• Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur | |