

Verwerkersovereenkomst Kindkans (versie 4.0 juni 2022)

Bijlage 2: beveiligingsbijlage

Burgemeester Jamessingel 2
2803 PD GOUDA
KvK 81749481
info@gouwe-academie.nl
www.gouwe-academie.nl

A. Maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, wijziging, opslag, toegang of openbaarmaking

I. Omschrijving van de maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Verwerking van Persoonsgegevens.

Gouwe Academie hanteert een autorisatiebeleid om te bepalen wie toegang moet hebben tot welke gegevens, zoals in de tabel hieronder aangegeven. Geautoriseerde medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

Medewerkers en gegevens:	Handelingen:
Helpdesk heeft waar nodig in opdracht van het samenwerkingsverband toegang tot persoonsgegevens.	Opsporen van oorzaken van foutsituaties om deze te herstellen en herhaling te voorkomen.

II. Omschrijving van de maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, Verwerking, toegang of openbaarmaking.

Organisatie van informatiebeveiliging en communicatieprocessen

- Gouwe Academie beschikt over een actief informatiebeveiligingsbeleid. Gouwe Academie heeft een security officer om risico's rond de verwerking van persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die toezien op naleving van het informatiebeveiligingsbeleid.
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- Gouwe Academie heeft procedures ingericht voor de behandeling van en communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers zijn geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- Gouwe Academie stimuleert bewustzijn, opleiding en training ten aanzien van informatiebeveiliging.
- Medewerkers hebben op grond van een autorisatiesystematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

B. Maatregelen om de Persoonsgegevens te beveiligen en continuïteit van de middelen, het netwerk, de server en de applicatie te waarborgen

Gouwe Academie heeft het Certificeringsschema van Edu-K gebruikt als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy voor Kindkans

(https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/). Hieronder staat de rapportage van de BIV- classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden.





Toetsvorm	Self-assessment
Uitvoerder toets	Educator B.V., Emil van den Berg, Lead engineer
Inlogpagina	https://start.kindkans.net
BIV-classificatie	Beschikbaarheid = L, Integriteit = M, Vertrouwelijkheid =H

Categorie	Maatregelen	Compliance	Uitleg
		<i>Voldaan/ Niet voldaan/ Alternatieve maatregel</i>	<i>Bij "Niet voldaan" aangeven hoe/wanneer dit wordt gecorrigeerd. Bij "Alternatieve maatregel" deze beschrijven.</i>
Beschikbaarheid	Ontwerp	Voldaan	
	Capaciteit beheer	Voldaan	
	Onderhoud	Gedeeltelijk voldaan	Wicket-techniek (frameworks) wordt momenteel vervangen.
	Testen	Voldaan	
	Monitoring	Voldaan	
	Herstel	Voldaan	
Integriteit	Herleidbaarheid (gebruikers)	Gedeeltelijk voldaan	Mogelijk maken wijzigingen terug te draaien; hier wordt nog niet aan voldaan.
	Back-up	Voldaan	
	Application controls	Voldaan	
	Onweerlegbaarheid	Gedeeltelijk voldaan	Logging als een gebruiker gegevens wijzigt; hier wordt nog niet aan voldaan.
	Herleidbaarheid (technisch beheer)	Voldaan	
	Controle integriteit	Voldaan	
	Acute dreigingen	Gedeeltelijk voldaan	Inbouwen van automatische detectie van verdacht netwerkverkeer; is nog niet gedaan.
Vertrouwelijkheid	Levenscyclus gegevens	Voldaan	
	Logische toegang	Voldaan	
	Fysieke toegang	Voldaan	
	Netwerktoegang	Voldaan	
	Scheiding omgevingen	Voldaan	
	Transport en fysieke opslag	Voldaan	
	Logging	Gedeeltelijk voldaan	Monitoren wanneer de logging wordt ingezien; hier wordt nog niet aan voldaan.
	Omgaan met kwetsbaarheden	Voldaan	

C. Afspraken over het informeren over beveiligingsincidenten en/of Datalekken

Gouwe Academie monitort 24/7 haar dienstverlening en heeft de in Bijlage 2 opgenomen maatregelen getroffen om ongeoorloofde of onrechtmatige toegang tot gegevens te voorkomen en te identificeren. Signalen die duiden op een datalek worden beoordeeld door de security officer van Gouwe Academie, die analyseert of sprake kan zijn van een Datalek. Indien er sprake is van een Datalek wordt de binnen Gouwe Academie gehanteerde datalekprocedure gevolgd.



De wijze waarop informatie wordt gedeeld:

Wanneer zich een Datalek voordoet, wordt de verwerkersverantwoordelijke door of namens Gouwe Academie zonder onredelijke vertraging na vaststelling dat sprake is van een Datalek per e-mail geïnformeerd.

Voor vervolgvragen of vragen kan telefonisch of per e-mail contact worden opgenomen met de helpdesk van Kindkans via de in de Privacy Bijsluiting opgenomen gegevens.

Gouwe Academie deelt ten minste de volgende informatie wanneer zich een Datalek voordoet:

- De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
- De oorzaak van het beveiligingsincident;
- De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
- Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
- De omvang van de groep betrokkenen;
- Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

Indien een concrete situatie zich daartoe leent, dan kan Gouwe Academie een (eerste) melding van een Datalek doen aan de Autoriteit Persoonsgegevens. Het Samenwerkingsverband wordt hierover geïnformeerd en blijft ook in dit geval eindverantwoordelijk voor de melding.

In geval van een (vermoeden van een) beveiligingsincident en/of Datalek, kan het Samenwerkingsverband in beginsel per e-mail contact met de Verwerker via onderstaande contactgegevens.

	Contactpersoon bij beveiligingsincidenten/Datalekken	Contactgegevens (e-mail en telefoonnummer)
Verwerker	Dhr. C.M. Codee	C.M.Codee@driestar-educatief.nl , (0182) 540333
Verwerker (bij afwezigheid)	Dhr. A.M. Vollmuller	a.m.vollmuller@gouwe-academie.nl (0182) 540333

Bijlage 2 (Beveiligingsbijlage) maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0, een initiatief van de PO-Raad, VO-raad, MBO Raad, de verschillende betrokken ketenpartijen (MEVW, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u op www.privacyconvenant.nl.