1.1 Bijlage 2

2. Beveiligingsbijlage

2.1 Omschrijving van de maatregelen zoals bedoeld in artikel 7 Verwerkersovereenkomst

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

Bureau ICE hanteert een autorisatiebeleid om te bepalen wie toegang moet hebben tot welke gegevens. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

Medewerkers en gegevens:	Handelingen:
Medewerkers van de klantenservice en sales hebben toegang tot licentieinformatie. Zij kunnen onder meer zien voor welke studenten een digitaal leermiddel is geactiveerd. De klantenservice en sales hebben inzage in leerresultaten van leerlingen.	Administratieve handelingen in het kader van de werking van meetinstrumenten en licenties. Ondersteuning van de eindgebruiker.
Analisten / deskundigen op het gebied van ontwikkeling van meetinstrument hebben toegang tot geanonimiseerde sets van resultaten van gebruik van meetinstrumenten, eventuele problemen/fouten bij gebruik	Analyse van het meetinstrument, gericht op verbetering van het materiaal, ontwikkeling en optimalisatie van (adaptief) meetinstrument, opsporing en verbetering van fouten in de werking van het digitale leermiddel.
IT-databasebeheerders hebben toegang tot de databases.	De handelingen van IT-databasebeheerders zijn gericht op continuïteit en optimalisatie van ICT-systemen.

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

- Bureau ICE beschikt over een actief informatiebeveiligingsbeleid.
- Bureau ICE heeft een coördinator voor informatiebeveiliging om risico's omtrent de verwerking van persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die zien op naleving van het informatiebeveiligingsbeleid.
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- Bureau ICE heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- Bureau ICE 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.

Beveiliging en continuïteit van de middelen, het netwerk, de server en de applicatie

Bureau ICE heeft het Certificeringsschema (zie https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/) gebruikt als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy voor TOA. Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden.

Organisatie	Bureau ICE		
Ict-toepassing	Toets.nl (TOA)		
Omschrijving	Toets-applicatie met toetsresultaten en leerlinggegevens		
Datum	2018-04-26		
Toetsvorm	Self-assessment		
Uitvoerder toets	Jacob Molenaar		
BIV-classificatie	(Beschikbaarheid=3, Integriteit=2, Vertrouwelijkheid=2)		
Categorie	**Maatregelen**	**Compliance**	**Uitleg**
		Voldaan/ niet voldaan/ alternatieve maatregel	(Bij niet voldaan aangeven hoe/wanneer dit wordt gecorrigeerd. Bij alternatieve maatregel deze beschrijven)
Beschikbaarheid	Overbelasting	Voldaan	
	Business continuity	Niet voldaan	Vertrouwelijk. Op aanvraag in te zien
	Ontwerp	Voldaan	
	Monitoring	Voldaan	
	Testen	Voldaan	
	Software	Voldaan	
	Actuele dreigingen	Voldaan	
Integriteit	Herleidbaarheid (gebruikers)	Voldaan	Vertrouwelijk. Op aanvraag in te zien
	Backup	Voldaan	
	Application controls	Voldaan	
	Onweerlegbaarheid	Voldaan	
	Herleidbaarheid (technisch beheer)	Voldaan	
	Controle integriteit	Voldaan	
	Onweerlegbaarheid	Voldaan	

	Actuele dreigingen	Voldaan	
Vertrouwelijkheid	Levenscyclus gegevens	Voldaan	
	Logische toegang	Niet Voldaan	Vertrouwelijk. Op aanvraag in te zien
	Fysieke toegang	Voldaan	
	Netwerk toegang	Voldaan	
	Scheiding omgevingen	Voldaan	
	Transport en fysieke opslag	Niet voldaan	Vertrouwelijk. Op aanvraag in te zien
	Logging	Niet voldaan	Vertrouwelijk. Op aanvraag in te zien
	Toetsing	Voldaan	
	Actuele dreigingen	Voldaan	

III. Omschrijving van de maatregelen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling.

De systemen van Bureau ICE worden jaarlijks gecontroleerd op veiligheid door Pine Digital Security of Nixu Corporation. Daarnaast voorziet het beveiligingsbeleid van Bureau ICE in interne processen om kwetsbaarheden te identificeren.

2.2 Rapportage

Verwerker actualiseert deze informatie voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via http://www.toets.nl/privacy-statement.

In het geval u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met de helpdesk van Bureau ICE via 0345 656 685 of per mail via privacy@bureau-ice.nl.

2.3 Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

- *De wijze waarop monitoring en identificatie van Datalekken plaatsvindt*

Bureau ICE 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 Bureau ICE, die analyseert of sprake kan zijn van een Datalek.

- *De wijze waarop informatie wordt gedeeld:*

Wanneer zich een Datalek voordoet, wordt de verwerkersverantwoordelijke onderwijsinstelling door of namens Bureau ICE in beginsel zonder onredelijke vertraging na vaststelling dat sprake is van een Datalek per e-mail geïnformeerd. Afhankelijk van de situatie, kan ook informatie worden gedeeld via onze website en officiële sociale media kanalen en/of officiële distributeurs en/of handelsagenten.

Voor vervolgacties of vragen kan telefonisch of per e-mail contact worden opgenomen met onze helpdesk via de in de Privacy Bijsluiter opgenomen gegevens.

- *Bureau ICE 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 Bureau ICE een (eerste) melding van een Datalek doen aan de Autoriteit Persoonsgegevens. De Onderwijsinstelling wordt hierover geïnformeerd en blijft ook in dit geval eindverantwoordelijk voor de melding.

2.4 Versie

Deze bijlage is voor het laatst bijgewerkt op 25 april 2018.

Onderwijsinstelling,	Verwerker, Bureau ICE
Naam:	Naam: Michiel Colenbrander
Functie:	Functie: Directeur
Datum:	Datum:
Handtekening:	Handtekening:

Deze privacy bijsluiter maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 3.0, een initiatief van de PO-Raad, VO-raad, MBO Raad, de verschillende betrokken ketenpartijen (GEU, KBB-e en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: http://www.privacyconvenant.nl.