Oplegnotitie: Certificeringsschema informatiebeveiliging en privacy ROSA v3.0 - advies Bureau Edustandaard

Voor:	Standaardisatieraad, Edustandaard
Van:	Bureau Edustandaard
Datum:	9 juni 2022
Betreft:	Oplegnotitie bij het advies en aanmeldformulier m.b.t. **Certificeringsschema informatiebeveiliging en privacy ROSA v3.0**

1. Samenvatting

De afspraak Certificeringsschema informatiebeveiliging en privacy ROSA v3.0 bestaande uit vier documenten (*"Algemene beschrijving", "Proces", "Toetsingskader" en "Toezicht"*) is namens de Edustandaard werkgroep Informatiebeveiliging en privacy (IBP) ingediend door Jordy van den Elshout, op 24 mei 2022 middels het Aanmeldformulier afspraak bij Edustandaard - Certificeringsschema informatiebeveiliging en privacy ROSA 2022.

Dit aanmeldformulier is namens Bureau Edustandaard verwerkt en beoordeeld door Jeroen Hamers (standaardisatie expert) en heeft geresulteerd in het volgende advies van bureau Edustandaard over de update van de afspraak Certificeringsschema informatiebeveiliging en privacy ROSA v3.0:

☑ Voldoende, met aandachtspunten (zie verderop in dit document hoofdstuk 3. Advies van bureau Edustandaard).

Dit advies is voor wederhoor voorgelegd aan de indiener. Reacties van de indiener zijn in de gedetailleerde uitwerking van het advies van Bureau Edustandaard opgenomen.

Voorafgaand aan de beoordeling door Bureau Edustandaard:

De afspraak is al sinds februari 2015 in beheer bij Edustandaard. Sindsdien zijn er naast deze meest recente versie nog twee andere versies verschenen (in juli 2017 en maart 2018).

2. Doel en Doelgroep

De afspraak is een gezamenlijk opgesteld ‘normenkader’, een baseline van maatregelen op het gebied van informatiebeveiliging voor organisaties die diensten – ondersteund door ict-toepassingen – leveren in de onderwijsketen.

Op basis van een voorgeschreven werkwijze bepaalt een leverancier een beveiligingsniveau. Aan dit beveiligingsniveau zijn specifieke maatregelen gekoppeld die gelden als een baseline waaraan de leverancier dan moet voldoen (comply) of een beargumenteerde afwijking voor moet geven (explain).

Er is een rapportageformat waardoor invullen en toetsen wordt vergemakkelijkt. Er zijn verschillende niveaus van toezicht gedefinieerd, van zelftoetsing tot externe audit. Daardoor hebben andere partijen inzicht in hoeveel vertrouwen gegeven kan worden aan de uitspraak van een leverancier dat deze aan het Certificeringsschema voldoet

Het doel van het Certificeringsschema is:

- Specificatie van een baseline van maatregelen op het gebied van informatiebeveiliging en privacy voor onderwijstoepassingen;
- Transparantie bieden over welke ICT-toepassingen voldoen aan deze baseline;
- Het creëren van een solide basisniveau van informatiebeveiliging voor alle geleverde ict-toepassingen in de onderwijsketen
- En, dit – bovengenoemde – zo gebruiksvriendelijk mogelijk te maken

Het certificeringsschema betreft maatregelen voor ict-toepassingen die binnen het onderwijs worden gebruikt, ongeacht welke sector.

3. Advies van bureau Edustandaard

Hieronder een samenvatting van de gedetailleerde uitwerking van het advies van Bureau Edustandaard.

Het bureau geeft het volgende advies:

✓ Voldoende, met aandachtspunten

2.1) Advies om het woord ‘periodiek’, overal waar het gebruikt wordt, nader te specificeren.
2.1) Overweeg de scope, genoemd in de beantwoording van het advies uit 2018 van Bureau Edustandaard (blz. 4), ook in de documentatie van de standaard op te nemen, bijvoorbeeld als aanvulling op de laatste alinea van paragraaf 1.5 van Certificeringsschema algemene beschrijving.
2.1) Zorg ook op de andere plaatsen in de overige documentatie dat de scope eenduidig wordt benoemd.
2.4) Gebruik in ieder document dezelfde indeling van mogelijke maateregelen, om eventuele verwarring te voorkomen.

Aanvullende adviezen, al wel met beoordeling ✓ **Goed**

1.1) Onderzoek of deze afspraak in een bredere scope toepasbaar is dan alleen de educatieve keten.
3.4) Overweeg om, ten behoeve van gebruikersgemak en daarmee snellere doorvoering van aangescherpte maatregelen, om een meer gedetailleerd overzicht van wijzigingen als bijlage toe te voegen (bijvoorbeeld zoals in het aanmeldformulier bij vraag 7.1 voor eerdere versies is gedaan).
3.4) Overweeg om de RFC’s te publiceren via de Edustandaard website.
3.5) Overweeg, ten behoeve van efficiënt en effectief beheer, om (eventueel ‘achter de schermen’) gebruik te maken van een totaaloverzicht van (deel)maatregelen, zodat teksten eenvoudiger consistent te houden zijn.

Overige constateringen

✓ Voldoende, met aandachtspunten

4.-Certificeringsschema_toetsingskader-v3.0-2.xlsx ☐ Onlogisch verschil dag/werkdag: Bij omschrijving van beschikbaarheid staat bij Middel “dag” en bij Hoog “werkdag” (andersom zou logischer zijn) ➢ **[!Beschikbaarheid$B$6] en [!Beschikbaarheid$B$7]** “Algeheel verlies of niet beschikbaar zijn van deze applicatie gedurende een dag/werkdag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.” ➢ **[!Beschikbaarheid$B$5],** bij Laag, wordt “meer dan een dag” gebruikt (zou dat dan niet ook “meer dan een werkdag” moeten zijn?)
☐ **Diverse tekstuele verbetersuggesties** (inclusief suggesties t.a.v. verwijzingen) (zie bijlage van advies)

Aanvullende adviezen, al wel met beoordeling ✓ **Goed**

1.-Certificeringsschema_algemene_beschrijving-v3.0.pdf , blz. 8: ☐ **Quote:** "Aanpassingen aan het toetsingskader, bijvoorbeeld wegens optreden van nieuwe risico's of bijstelling van de maatregelen, worden direct gepubliceerd. Hiermee wordt een uitzondering gemaakt op het gebruikelijke standaardisatie proces. Jaarlijks wordt de standaard als geheel, dus toetsingskader en de overige onderdelen van het certificeringsschema, opnieuw formeel vastgesteld." ☐ **Vraag:** Kunnen betrokken partijen zich hierover automatisch op de hoogte laten stellen (bijvoorbeeld via RSS-feed of nieuwsbrief)?
2.-Certificeringsschema_proces-v3.0.pdf, blz. 5, §2.1: ☐ **Quote:** "Tip: sommige organisaties kiezen om de eerste keer niet elke applicatie in detail te analyseren, maar ze te groeperen in typen applicaties. Daardoor kunnen detailanalyses van specifieke applicaties leren van voorgaande analyses en kost het toepassen van het certificeringsschema elke opeenvolgende keer minder inspanning" ☐ **Advies:** Overweeg hier ook een tip over prioritering aan toe te voegen. In §5.1 staat immers ook al iets over prioritering, deze eerste prioritering zou de latere prioritering moeten versterken en niet tegenwerken.

Gebruiksadvies:

- "Verplicht" ("Voor deze standaarden geldt het 'Pas toe of leg uit'-beleid.")
- ~~"Aanbevolen" ("Deze standaarden zijn niet verplicht, maar net zo nuttig.")~~

In de huidige praktijk van Edustandaard krijgen de afspraken met een breed toepassings- en werkingsgebied die vaak ook een ontstaan hebben vanuit de PTOLU-lijst van Forum Standaardisatie, het gebruiksadvies "Verplicht". Het gaat om afspraken zoals: RIO canonieke modellen, alle UBV-afspraken, Edukoppeling. Certificeringsschema 3.0 hoort naar de mening van Bureau Edustandaard ook in dit rijtje thuis: naast een breed toepassings- en werkingsgebied betreft het enerzijds een noodzakelijk te gebruiken afspraak (BIV-risico's moeten deels op basis van wetgeving in kaart zijn gebracht) en anderzijds is dit het meest voor de hand liggende instrument dat in de onderwijsketens beschikbaar is. Het heeft zijn waarde inmiddels bewezen, en het bevordert een uniforme werkwijze in de ketens. De Architectuurraad ondersteunt in haar bijeenkomst van 14 april bovenstaande en acht het van groot belang dat het gebruik vanzelfsprekend wordt (zie expliciete vraag aan de Standaardisatieraad). Aanvullend wordt nog vermeld dat in de Leermiddelenketen het gebruik hiervan ook wordt verwacht: het Privacy Convenant 4.0 van Edu-K is geënt op deze nieuwe versie van het Certificeringsschema. Tot slot: dit gebruiksadvies biedt alle ruimte om af te wijken, echter dan is wel een uitleg aan de keten verschuldigd.

Bureau Edustandaard stelt daarom in samenspraak met de Architectuurraad voor om het gebruiksadvies "Verplicht" *('pas toe of leg uit')* mee te geven.

4. Advies werkgroep informatiebeveiliging en privacy (IBP)

De werkgroep geeft een positief advies over de inbeheername van de standaard om de volgende redenen:

- In deze versie (2022) is het Toetsingskader grondig herzien en is het functioneel uitgebreid.
- Qua vorm zijn de vragen voor classificatie nu onderdeel van het Toetsingskader, zodat op basis daarvan direct de juiste maatregelen worden getoond.
- Ook wordt de rapportagevorm automatisch opgemaakt.
- Qua inhoud zijn de vragen en maatregelen verduidelijkt.
- De maatregelen zijn in sommige gevallen ook aangescherpt. Onder andere om
    a) aan te sluiten bij de huidige stand van techniek en het huidige dreigingsbeeld, zoals voor de back-upinrichting en minimaal 2FA voor beheertoegang; en
    b) om preciezer te zijn in verantwoordelijkheden van de leverancier (de verwerker).
- Op basis van het nieuwe Toetsingskader zijn de begeleidende teksten zoals de 'Algemene beschrijving', 'Proces' en 'Toezicht' bijgewerkt.
- Daarnaast is er een nieuwe versie van Privacy Convenant gepubliceerd, waarin verwezen wordt naar de nieuwe versie van deze afspraak. Het is van belang dat gebruikers van het Privacy Convenant deze goedgekeurde afspraak kunnen gebruiken.

5. Advies Architectuurraad

Op 14 april 2022 is tijdens de Architectuurraadbijeenkomst, middels een presentatie van Jordy van den Elshout namens de werkgroep IBP, advies gevraagd over inbeheername van de nieuwe versie van de afspraak. De Architectuurraad kwam tot de volgende besluiten (zie agendapunt 4 van de notulen):

- De Architectuurraad adviseert positief over het nieuwe Certificeringsschema ROSA 2022.
- **Actiepunt:** De Standaardisatieraad wordt gevraagd hoe het gebruik in de onderwijsketens flink kan worden gestimuleerd.

6. Roadmap

De werkgroep hanteert sinds 2017 een nieuwe werkwijze waarbij RFC's worden ingediend en per bijeenkomst worden behandeld en (eventueel) gewijzigd worden goedgekeurd.

Er zijn geen verdere grote ontwikkelingen gepland.

De afspraak wordt reeds breed gebruikt binnen de leermiddelenketen, middels het privacy convenant. Ook wordt het door de schoolbesturen gebruikt ter toetsing van onderwijs toepassen, echter is niet bekend hoe breed.

Wel is tijdens de architectuurraad besproken of de standaard breder gebruikt moet worden binnen de onderwijssector, wat ook een bespreekpunt is voor de standaardisatieraad. Met name om toetsing ervan te kunnen bevorderen.

7. Gevraagd besluit

7.a

☑ **Voldoende, met aandachtspunten**

De leden van de Standaardisatieraad wordt gevraagd om, gelet op bovenstaande overwegingen:

- In te stemmen met de inbeheername van de update van de afspraak "**Certificeringsschema informatiebeveiliging en privacy ROSA", versie 3.0**.
- Het gebruiksadvies is daarbij "Verplicht" *("Voor deze standaarden geldt het 'Pas toe of leg uit'-beleid.")*.
- Het certificeringsschema betreft maatregelen voor ict-toepassingen die binnen het onderwijs worden gebruikt, ongeacht welke sector.

7.b

- Daarnaast worden de leden van de Standaardisatieraad door de leden van de Architectuurraad gevraagd **"hoe het gebruik in de onderwijsketens flink kan worden gestimuleerd."**