Edustandaard

Werkgroep IBP – Certificeringschema IBP ROSA

Nieuwe versie

Update tijdens Architectuurraad

14 april 2022

edustandaard

Certificeringsschema Informatiebeveiliging en Privacy ROSA

Het is:

- Een baseline voor informatiebeveiliging van toepassingen in het onderwijs
- Gebaseerd op ISO 27001
- In publiek private samenwerking tot stand gekomen

Van toepassing op alle toepassingsgebieden binnen het PO, VO, MBO en HO:

- Leveranciers kunnen er eenvoudig mee aantonen dat hun toepassing voldoet aan de relevante informatiebeveiligingseisen.
- Onderwijsinstellingen kunnen eenvoudig nagaan of een ict-toepassing voldoet aan de relevante informatiebeveiligingseisen.

Certificeringsschema Informatiebeveiliging en Privacy ROSA

Bestaat uit drie onderdelen:

1. Een classificatiehulpmiddel om de mate van belang van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) te bepalen.
2. Een toetsingskader met verschillende informatiebeveiligingsmaatregelen per BIV-niveau. Hogere B, I of V classificatie geeft zwaardere maatregelen.
3. Rapportage hulpmiddel o.b.v. pas toe of leg uit

Nieuwe versie van het Certificeringschema, versie 3.0

- Het certificeringsschema wordt periodiek herzien. Daarom is de werkgroep IBP in juni 2021 bijeengekomen voor een herziende versie.
  - Na 7 bijeenkomsten en een aantal voorbereidende werksessies, is zowel de inhoud herzien en de vorm vernieuwd.

- Parallel loopt ook de vernieuwing van het Privacyconvenant, met de bijbehorende Model Verwerkersovereenkomst.
  - In bijlage 2 wordt het Certificeringschema gebruikt t.b.v. verklaring informatiebeveiliging. Bij de publicatie van deze nieuwe versie is het van belang dat ook de nieuwe versie van het Certificeringschema beschikbaar is.

Inhoud is verduidelijkt en aanscherpt

De vragen voor het bepalen van de BIV (het Classificatieschema) en de bijbehoren maatregelen per beveiligingsniveau (het Toetsingskader) zijn herzien.

1. De vragen zijn met name verduidelijkt; naar verwachting heeft dit nauwelijks impact op de uitkomst: de BIV-classificatie.
2. De maatregelen zijn ook hoofdzakelijk verduidelijkt, maar in sommige gevallen ook aanscherpt
   a) Om aan te sluiten bij de huidige stand van techniek en het huidige dreigingsbeeld, zoals voor de back-upinrichting en min. 2FA voor beheertoegang.
   b) Om preciezer te zijn in verantwoordelijkheden van de leverancier (de verwerker)
   c) Verwachting is dat de maatregelen in de praktijk weinig aangepast hoeven te worden, maar gebruiksgemak wel is toegenomen.

Vorm is aangepast voor de gebruiksvriendelijkheid

De werkgroep heeft tijdens de laatste bijeenkomst gekozen om de Classificatie en het Toetsingskader incl. rapportage samen te voegen.

1. Hierdoor is het mogelijk om op basis van de antwoorden, direct de betreffende maatregelen te tonen die nodig zijn op basis van de BIV-classificatie.
2. Ook is het mogelijk om de status per implementatie te noteren, waarmee automatisch het rapport voor bijlage 2 van het Privacyconvenant wordt genereerd. Deze kan 1-op-1 geplakt worden in bijlage 2.
3. Daarnaast
   i. Zijn de BIV-niveaus aangepast naar Laag, Midden, Hoog i.p.v. 1, 2, 3.
   ii. En zijn de maatregelcategorieën in een logische volgorde gezet.

Voorgestelde stappen

Het classificatieschema kent twee stadia van versies: ‘Vastgesteld’ en ‘Meest recente versie’. De nieuwe versie staat online als ‘meest recente versie’. Gebruikers van het Certificeringschema hebben hierdoor de mogelijk om de nieuwe (gebruiksvriendelijke) versie te gebruiken bij herziening van hun verwerkersovereenkomsten.

Nu: verder afmaken van het Certificeringsschema, zoals begeleidende tekst en pagina op Edustandaard. Op basis daarvan kan het ter vaststelling voorgelegd worden aan de Standaardisatieraad.

Kan de Architectuurraad zich hierin vinden?