

Certificeringsschema informatiebeveiliging en privacy ROSA (concept onder Edustandaard)



Verwachting eind
september 2016

Verantwoording

Bron:

ROSA

Augustus 2016

ROSA

ROSA is de Referentie Onderwijs Sector Architectuur, de referentiearchitectuur voor het onderwijsdomein die zich richt op informatieketens en (onderwijs) sector overstijgende aspecten van informatievoorziening. De ROSA heeft als doel de informatievoorziening binnen het onderwijsdomein te optimaliseren. Hiervoor is samenwerking tussen organisaties essentieel. Scholen, de overheid en derden werken in toenemende mate samen in ketens, een goede informatie-uitwisseling is hierbij essentieel.

Bewerkt door:

Kennisnet / saMBO-ICT

Auteurs

Leo Bakker (Kennisnet)

Ludo Cuijpers (Kennisnet)

Axel Eissens (Kennisnet)

Augustus 2016

Sommige rechten voorbehouden

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgever van Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.

Creative commons

Naamsvermelding 3.0 Nederland
(CC BY 3.0)



De gebruiker mag:

- Het werk kopiëren, verspreiden en doorgeven
- Remixen – afgeleide werken maken

Onder de volgende voorwaarde:

- Naamsvermelding – De gebruiker dient bij het werk de naam van Kennisnet te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

Korte inleiding

Als mbo instelling ben je opdrachtgever en moet je duidelijke afspraken maken. Ook op het gebied van informatiebeveiliging en privacy.

Met een leverancier spreek je minimaal drie dingen af:

- Welke BIV-classificatie wordt gehanteerd:
 - o spreek af welk classificatieschema gehanteerd wordt, óf
 - o spreek af hoe de BIV-classificatie van de mbo instelling zich verhoudt tot de classificatie van de leverancier.
- Wat wordt verstaan onder passende/adequate maatregelen:
 - o spreek af welke standaard of welke normenkader wordt gehanteerd voor het bepalen van passende maatregelen;
 - o spreek bijvoorbeeld af welke maatregelen horen bij een hoge vertrouwelijkheid.
- Hoe maatregelen getoetst worden:
 - o door het opvragen van een (onafhankelijke) verklaring of certificering bij aanvang;
 - o door het regelmatig – minimaal jaarlijks – (laten) uitvoeren van een toets of audit tijdens de relatie.

Het certificeringsschema informatiebeveiliging en privacy ROSA bevat deze onderdelen, maar is nog in concept-fase. Het certificeringsschema kan alsnog gebruikt worden, maar daar moet de mbo instelling het met de leverancier over eens worden. Het is ook mogelijk om ISO 27001/27002 te gebruiken, of soortgelijke standaarden of normenkaders. Hou hierbij wel bovenstaande aspecten in het achterhoofd.

Verwijzing naar documenten ROSA

<https://www.edustandaard.nl/standaarden/afspraken/afpraak/certificeringsschema/2.0/>

Bijlage: Framework informatiebeveiliging en privacy in het mbo

Mbo ibp architectuur (IBPDOc4)	Verantwoordingsdocument informatiebeveiliging en privacy in het mbo onderwijs (IBPDOc1)								Privacy compliance kader mbo (IBPDOc2B) Normenkader informatiebeveiliging mbo (IBPDOc2A)
	Mbo roadmap informatiebeveiligings- en privacy beleid (IBPDOc5)								
	Model informatiebeveiligings- en privacy beleid voor de mbo sector (IBPDOc6)								
	Toetsingskader informatiebeveiliging: clusters 1 t/m 6 (IBPDOc3)				Toetsingskader privacy: cluster 7 (IBPDOc7)				
	Toetsingskader examinering pluscluster 8 IBPDOc8	Tk digitaal ondertekenen pluscluster 9 IBPDOc9	Toetsingskader vmbo-mbo pluscluster 10 IBPDOc10	Benchmark mbo sector IBPDOc11	Functie-waardering ibp IBPDOc12	Positionering ibp IBPDOc13	Risico inventarisatie ibp IBPDOc29		
	Handleiding BIV classificatie IBPDOc14	BIV en PIA bekostiging IBPDOc15	BIV en PIA indiensttreding IBPDOc16	BIV en PIA online leren IBPDOc17	Bewerkers-overeenkomst mbo versie IBPDOc18	Certificeringsschema ibp ROSA IBPDOc19			
	Starterkit identity mngt mbo versie IBPDOc22	Starterkit rbac mbo versie IBPDOc23	Starterkit bcm mbo versie IBPDOc24	Integriteit-code mbo versie IBPDOc25	Acceptable use policy mbo versie IBPDOc26	Responsible disclosure mbo versie IBPDOc27			
	Implementatievoorbeelden van kleine en grote instellingen				Technische quick scan, APK (IBPDOc30)				
	Handboek mbo-audits (IBPDOc21)								
	Hoe? Zo! Informatiebeveiligingsbeleid in het mbo				en Hoe? Zo! Privacy in het mbo				
		ibp mbo		voorbeelden		ibp ho (SCIPR)			