Kennisnet

Informatiebeveiliging binnen Edustandaard

Standaardisatieraad 19 mei 2016

Dirk Linden - CTO Kennisnet

Vragen?

- Hoe wordt de aansluiting tussen informatiebeveiliging en privacy geborgd?
- Welke rol ligt bij edustandaard en welke rol ligt bij andere partijen?

Kennisnet

Informatiebeveiliging en Privacy

- Informatiebeveiliging levert maatregelen om privacy te borgen.
- Principes tav Informatiebeveiliging en Privacy al opgenomen in het ROSA katern ‘Privacy en Beveiliging’
- Privacy is verankerd in de wet en het heeft dus geen zin om daar binnen het onderwijs een eigen standaard voor te ontwikkelen.
- De implementatie van privacy is wel iets waar (keten)afspraken over worden gemaakt.
- Over informatiebeveiliging worden (keten)afspraken gemaakt, o.a. via het Certificeringsschema

Kennisnet

Beknopt overzicht Privacyafspraken:

Alle afspraken in lijn met de principes uit het ROSA katern IBP

	PO-VO	MBO [1)]	HO
Instelling	Privacyconvenant [Edu-K]	Framework IBP: [Taskforce IBP] * Compliancekader privacy (IBPDOC 2b) * Toetsingskader privacy (IBPDOC7) * eventueel nader te bepalen toetsingskader voor leveranciers (vgl. privacyconvenant)	Juridisch normenkader cloudservices hoger onderwijs [Juridische commissie Surfnet]
Afdwingbaarheid bij Leveranciers	Model bewerkersovereenkomst met bijlages: A) Privacybijsluiter B) Technische en organisatorisch beveiligingsmaatregelen (met daarin de verplichting zich te conformeren aan het Certificeringsschema)	Voorlopig: * leermiddelen: bewerkersovereenkomst (gebaseerd op model po/vo) * Overig zoals MS, Google: SURF-modelbewerkersovereenkomst	SURF-modelbewerkersovereenkomst
Aantoonbaar compliant	Verklaring ondertekening privacyconvenant (centraal register bij privacyconvenant.nl)	Individuele ondertekening bewerkersovereenkomst	Individuele ondertekening bewerkersovereenkomst
Toetsbaar	In onderzoek: Toetsing bewerkersovereenkomsten Interne audits o.b.v. Toetsingskader CS (in 2016)		Externe audit o.b.v. TPM verklaring

Kennisnet

Voorstellen

Om de relatie tussen informatiebeveiliging en privacy binnen edustandaard expliciet te beleggen:

- Naamgeving: Katern ‘Privacy en Beveiliging’ wordt ‘Katern IBP’

- Edustandaard ‘Werkgroep Informatiebeveiliging’ wordt ‘Werkgroep IBP’ en krijgt als opdracht mee om architectuur principes van de principes uit het katern IBP. (Principes al benoemd nu architectuurrichtlijnen)

Informatiebeveiliging en Privacy

- Informatiebeveiliging levert maatregelen om privacy te borgen.
- Principes tav Informatiebeveiliging en Privacy al opgenomen in het ROSA katern ‘Privacy en Beveiliging’
- Privacy is verankerd in de wet en het heeft dus geen zin om daar binnen het onderwijs een eigen standaard voor te ontwikkelen.
- De implementatie van privacy is wel iets waar (keten)afspraken over worden gemaakt.
- Over informatiebeveiliging worden (keten)afspraken gemaakt, o.a. via het Certificeringsschema

Beknopt overzicht informatiebeveiligingsnormen onderwijssectoren

Alle afspraken in lijn met de principes uit het ROSA katern IBP

	PO-VO	MBO	HO
Instelling	In ontwikkeling – [Kennisnet in opdracht van PO en VO-raad]	Normenkader MBO – [Taskforce IBP MBO]	Normenkader Informatiebeveiliging HO 2015 - [SURFnet]
	X	Peer audits o.b.v. Toetsingskader MBO	Peer audits o.b.v. Toetsingskader HO
Leveranciers	Certificeringsschema bestaande uit: • Normenkader • Toetsingskader (TKI) • Toezichtskader (voorlopig interne audits) [Edustandaard werkgroep IBP]	Juridisch Normenkader Cloudservices – [Juridische commissie Surfnet]	
	Interne audits o.b.v. Toetsingskader CS (in 2016)	Externe audit o.b.v. TPM verklaring	

Kennisnet

Certificeringschema

Heeft als doel:

- Specificatie van een baseline van maatregelen op het gebied van informatiebeveiliging en privacy;
- Transparantie bieden over welke organisaties voldoen aan deze baseline;
- Het creëren van een solide basisniveau van informatiebeveiliging voor alle geleverde ict-diensten in de onderwijsketen.

Kennisnet

Certificeringschema

Bestaat uit:

- Een algemene omschrijving (met verwijzing naar het gebruikte ISO2700x kader)
- Een roadmap; dit beschrijft beheer en doorontwikkeling.
- Een procesdocument; dit beschrijft de toepassing van het Certificeringsschema voor een enkele organisatie.
- Een classificatiehulpmiddel; deze helpt een organisatie om het gewenste niveau van informatiebeveiliging te bepalen.
- Een toetsingskader; de helpt een organisatie en/of auditor om te toetsen of de juiste maatregelen zijn getroffen op basis van de classificatie.
- Een toezichtdocument; dit beschrijft verschillende niveaus van audit op het toetsingskader en ondersteunt zowel de organisatie als de onderwijsinstelling.

Certificeringsschema

Classificatie	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Situatie A	2	1	1
Situatie B	2	2	3
Situatie C	3	4	3
…	4	3	4

Beschikbaarheid	Mens	Techniek	Proces
1			
2			
3			
4			

Integriteit	Mens	Techniek	Proces
1			
2			
3			
4			

Vertrouwelijkheid	Mens	Techniek	Proces
1		Maatregel k	
2	Maatregel a		Maatregel x
3	*Maatregel b*	*Maatregel l*	*Maatregel y*
4	Maatregel c	Maatregel m	Maatregel z

Kennisnet

Certificeringsschema: Wat gebeurt waar?

Prinicpes (waarom)	Afspraken (wat)	Implementatie (hoe)
ROSA	Certificeringsschema	Implementatieplan
Edustandaard	**Edustandaard**	**Edu-K**
Standaardisatieraad ▪ Bestuurlijke vaststelling door o.a. sectorraden en brancheorganisaties	**Standaardisatieraad** ▪ Bestuurlijke vaststelling door o.a. sectorraden en brancheorganisaties	**Edu-K** ▪ Vaststellen implementatiekaders ▪ Vaststellen toezicht
Architectuurraad ▪ Samenhang met architectuur ▪ Samenhang met andere processen (vb Edukoppeling, OSO)	**Werkgroep** ▪ Ontwikkeling en beheer certificeringsschema	**Tactisch overleg Continuïteit en beveiliging** ▪ Implementeren van certificeringsschema (obv risicoanalyse) ▪ Afspraken over toezicht

Kennisnet

Bedankt voor uw aandacht

Dirk Linden
CTO

E-mail: d.linden@kennisnet.nl