Risicobeoordeling en -behandeling

2025-2029

Versieblad

Documenttitel	Risicobeoordeling en -behandeling 2025-2029
Versie	1.0
Datum	18-03-2024
Status	Definitief
Classificatie	Openbaar
Proceseigenaar	A.Verwijst, Privacy en Security Officer
Documentbeheerder	A.Verwijst, Privacy en Security Officer

Wijzigingshistorie			

Inhoud

1.	**Inleiding**	**4**
1.1	Aanleiding	4
1.2	Doel, scope en gebruikers	4
2.	**Risicobeoordeling en risicobeoordelingsmetholdologie**	**5**
2.1	Het proces	5
2.2	Het bepalen van de risico-eigenaren	5
2.3	Impact en waarschijnlijkheid (Kans)	5
2.4	Risicoacceptatiecriteria	6
2.5	Risicobehandeling	7
2.6	Regelmatige evaluaties van risicobeoordeling en risicobehandeling	7
2.7	Verklaring van toepasselijkheid en risico behandelingsplan	7
2.8	Berichtgeving	8
3.	**Beheer van de gegevens die op basis van dit document worden bijgehouden**	**9**
4.	**Validiteits- en documentbeheer**	**10**

1. Inleiding

1.1 Aanleiding

Informatiebeveiliging en het beschermen van persoonsgegevensbescherming zijn essentieel in het funderend onderwijs. Als Stichting Optimus Primair Onderwijs zijn we ons bewust van het belang van het veilig en zorgvuldig beheren van vooral persoons gegevens. Risico's zijn onvermijdelijk, maar door een evenwichtige afweging van risico's, maatregelen, uitvoerbaarheid en onderwijsbelang, streven we naar de bescherming van de beschikbaarheid, integriteit en vertrouwelijkheid van onze informatie. Bovendien is het van belang om veerkracht te integreren in onze beveiligingsstrategieën.

Voor de beveiliging van onze digitale en papieren documenten, software, personeel, computers, netwerken en externe processen, is het essentieel dat we gerichte maatregelen nemen. Een voorafgaande risicoanalyse helpt ons om deze risico's effectief te identificeren en te reduceren tot een aanvaardbaar niveau voor onze organisatie. We gebruiken hiervoor een specifiek Informatie Risicomanagement Framework.

1.2 Doel, scope en gebruikers

Dit document heeft als doel de manier waarop we bij Stichting Optimus Primair Onderwijs informatiebeveiligingsrisico's beoordelen en behandelen vast te leggen. We beschrijven welk risiconiveau acceptabel is volgens het Normenkader Informatiebeveiliging en Privacy Funderend Onderwijsnformatiebeveiliging.

We passen risicobeoordeling en risicobehandeling toe op alles in ons Information Security Management System (ISMS), dat wil zeggen op alle middelen die we in de organisatie gebruiken of die invloed kunnen hebben op de beveiliging van informatie in het ISMS.

Dit document is bedoeld voor alle medewerkers van Stichting Optimus Primair Onderwijs die betrokken zijn bij het beoordelen en behandelen van risico's.

2. Risicobeoordeling en risicobeoordelingsmetholdologie

2.1 Het proces

Het risicobeoordelings- en risicobehandelingsproces volgens paragraaf 2.1 hanteert een systematische aanpak binnen het Information Security Management System (ISMS). Belangrijke aspecten zoals documenten, software, personeel, computers, netwerken en externe diensten worden eerst geïdentificeerd. Daarna worden potentieel gevaar en kwetsbaarheden bij deze aspecten onderzocht. De Security Officer coördineert deze beoordeling, samen met de IT-afdeling, terwijl het College van Bestuur risico's evalueert op gevolgen en waarschijnlijkheid. De risico's worden in kaart gebracht met de 'Kans x Impact'-tabel uit paragraaf 2.3

2.2 Het bepalen van de risico-eigenaren

Voor elk risico moeten we een verantwoordelijke aanwijzen, dat is degene die de verantwoordelijkheid draagt voor dat specifieke risico. Dit kan dezelfde persoon zijn als de eigenaar van de betrokken zaak, maar dat hoeft niet per se zo te zijn.

2.3 Impact en waarschijnlijkheid (Kans)

Nadat we de personen verantwoordelijk voor de risico's hebben vastgesteld, is het belangrijk om de gevolgen te evalueren voor elk geval waarbij een dreiging en een kwetsbaarheid samenkomen en van invloed zijn op een specifieke zaak, als zo'n risico zich voordoet.

We bepalen het risico op basis van hoe ernstig de zwakte is en de waarschijnlijkheid dat deze wordt benut. Het risico wordt bepaald volgens de formule: **Kans x Impact = Risico**

		kans		
	risico matrix	laag	middel	hoog
impact	laag	laag risico	laag risico	middel risico
	middel	laag risico	middel risico	hoog risico
	hoog	middel risico	hoog risico	hoog risico

		kans		
	risico matrix	laag	middel	hoog
impact	laag	laag risico	laag risico	middel risico
	middel	laag risico	middel risico	hoog risico
	hoog	middel risico	hoog risico	hoog risico

Laag impact	0	Het verlies van vertrouwelijkheid, beschikbaarheid of integriteit heeft **geen impact** op de financiën, wettelijke verplichtingen, contracten of reputatie van de organisatie.
Matig impact	1	Het verlies van vertrouwelijkheid, beschikbaarheid of integriteit leidt tot **extra kosten en heeft een beperkte tot gematigde invloed** op wettelijke verplichtingen en de reputatie van de organisatie.
Hoge impact	2	Het verlies van vertrouwelijkheid, beschikbaarheid of integriteit heeft **aanzienlijke en/of onmiddellijke impact** op de financiën, bedrijfsvoering, wettelijke verplichtingen en de reputatie van de organisatie.

Na het beoordelen van de impact is het noodzakelijk om te kijken naar de kans dat een dergelijk risico zich voordoet, dat wil zeggen, de waarschijnlijkheid dat een dreiging gebruik zal maken van de zwakke plek van het betreffende activum

Lage kans	0	De huidige **beveiligingsmaatregelen** zijn **robuust** en hebben tot dusver voldoende bescherming geboden. We voorzien geen nieuwe incidenten in de toekomst.
Matige kans	1	De huidige **beveiligingsmaatregelen** zijn **matig**, en ze bieden over het algemeen een redelijke bescherming. Er is een kans op nieuwe incidenten, maar deze is niet bijzonder hoog.
Grote kans	2	De bestaande **beveiligingsmaatregelen** zijn **zwak** of ineffectief. Er bestaat een aanzienlijke kans dat dergelijke incidenten zich in de toekomst zullen voordoen.

Het risiconiveau wordt automatisch berekend door de waarden van impact en waarschijnlijkheid in de risicobeoordelingstabel in te vullen en deze twee waarden bij elkaar op te tellen. De bestaande beveiligingsmaatregelen moeten worden ingevuld in de laatste kolom van de risicobeoordelingstabel.

2.4 Risicoacceptatiecriteria

Acceptatie van een risico vindt plaats door de risico-eigenaar op basis van de risicowaarde in combinatie met de risicobereidheid:

1	De risico’s met Risicoklasse Laag worden geaccepteerd. Dit betreft waarde 0 en 1.
2	De risico’s met Risicoklasse Middel worden geaccepteerd als er geen tegenmaatregelen mogelijk zijn, of als de mogelijke tegenmaatregelen te duur zijn, in relatie tot het risico. Dit betreft waarde 2.
3	Voor de risico’s met Risicoklasse Hoog worden (aanvullende) maatregelen getroffen. Dit betreft de waarde 3 en 4.

Bij het nemen van maatregelen maken we een zorgvuldige afweging tussen de kosten van mogelijke acties in relatie tot de vermindering van risico's (kosten-batenanalyse). We voegen de gekozen maatregelen toe aan de lijst van beheersmaatregelen in ons gehele Information Security Management System (ISMS). We kiezen maatregelen die het risico voor de organisatie voldoende verminderen, zonder dat de kosten hoger zijn dan de voordelen. Eventuele resterende risico's moeten worden goedgekeurd door de directie.

2.5 Risicobehandeling

Geïdentificeerde onaanvaardbare risico's worden overgebracht van de risicobeoordelingstabel naar de risicobehandelingstabel. De Privacy en Security Officer leidt dit proces en houdt toezicht op de voortgang van de risicobehandeling.

Een of meer behandelingsopties moeten worden geselecteerd voor risico's met een waarde van 3 en 4:

1	Keuze van beveiligingscontrole of -controles van de ISO/IEC 27001-norm of andere beveiligingscontroles
2	Overdracht van de risico's aan een derde partij – bijvoorbeeld door een verzekeringspolis af te sluiten of een contract te sluiten met leveranciers of partners
3	Het risico vermijden door een bedrijfsactiviteit te staken die een dergelijk risico veroorzaakt
4	Het risico accepteren – deze optie is alleen toegestaan als de selectie van andere risicobehandelingsopties meer zou kosten dan de potentiële impact als een dergelijk risico zich zou voordoen

Het selecteren van de opties wordt uitgevoerd via de Risicobehandelingstabel. Meestal wordt optie 1 gekozen, waarbij een of meerdere beveiligingsmaatregelen worden geselecteerd. Als er meerdere maatregelen worden gekozen voor een risico, worden er extra rijen toegevoegd onder de rij waarin het risico wordt vermeld.

Voor risico's met betrekking tot uitbestede processen moeten we de kwestie aanpakken via de contracten met de verantwoordelijke derden, zoals beschreven in het inkoopbeleid.

In het geval van optie 1 (selecteren van beveiligingsmaatregelen) moeten we de nieuwe waarden voor de gevolgen en de waarschijnlijkheid in de Risicobehandelingstabel beoordelen om de effectiviteit van de geplande maatregelen te evalueren.

2.6 Regelmatige evaluaties van risicobeoordeling en risicobehandeling

Risicoverantwoordelijken moeten regelmatig de bestaande risico's beoordelen en de Risicobeoordelingstabel en Risicobehandelingstabel bijwerken wanneer er nieuwe risico's worden geïdentificeerd. Deze beoordeling vindt minstens één keer per jaar plaats, maar kan vaker nodig zijn als er belangrijke organisatorische veranderingen, technologische wijzigingen, aanpassing van zakelijke doelen, of veranderingen in de zakelijke omgeving optreden.

2.7 Verklaring van toepasselijkheid en risico behandelingsplan

In de Verklaring van Toepasselijkheid (V.v.T.) geven we als Stichting Optimus Primair Onderwijs aan welke beveiligingsmaatregelen uit de ISO/IEC 27001-norm worden gebruikt en welke niet, en waarom. We geven ook aan of deze maatregelen daadwerkelijk in gebruik zijn.

- Namens de personen die verantwoordelijk zijn voor de risico's, accepteert het College van Bestuur (C.v.B.) de resterende risico's via de Verklaring van Toepasselijkheid.
- De Privacy en Security Officer zal een plan opstellen en/of opdracht geven om de maatregelen uit te voeren, en dit plan wordt goedgekeurd door het College van Bestuur en is risico-eigenaar.

2.8 Berichtgeving

De Privacy en Security Officer zal de resultaten van risicobeoordeling en risicobehandeling, en alle daaropvolgende beoordelingen, documenteren in het risicobeoordelings- en behandelingsrapport.

De Privacy en Security Officer zal de voortgang van de implementatie van het Riskbehandelplan volgen en de resultaten elke kwartaal rapporteren aan het CvB.

3. Beheer van de gegevens die op basis van dit document worden bijgehouden

Recordnaam	Opslaglocatie	Persoon die verantwoordelijk is voor de opslag	Controle voor record-beveiliging	Bewaartermijn
Risicobeoordelings-tabel (elektronisch formulier – Excel-document).	MS-Teams-omgeving, Kanaal: *Informatie en beveiliging*	Privacy en Security Officer	Alleen Privacy en Security Officer heeft het recht om in te schrijven in en wijzigingen aan te brengen in de risicobeoordelings-tabel.	Gegevens worden permanent opgeslagen.
Risicobehandelingsta-bel (elektronisch formulier – Excel-document).	MS-Teams-omgeving, Kanaal: *In-formatie en beveiliging.*	Privacy en Security Officer	Alleen Privacy en Security Officer heeft het recht om in te schrij-ven in en wijzigingen aan te brengen in de Risicobehandelingstabel.	Gegevens worden permanent opgeslagen.
Risicobeoordeling en behandelingsrapport (elektronisch formulier – PDF-formaat).	MS-Teams-omgeving, Kanaal: *In-formatie en beveiliging*.	Privacy en Security Officer	Het rapport is opgesteld in alleen-lezen PDF-formaat.	Het verslag wordt bewaard voor een periode van 3 jaar.
Verklaring van toepasselijkheid (elektronisch formulier – PDF-formaat).	MS-Teams-omgeving, Kanaal: *In-formatie en beveiliging* .	Privacy en Security Officer	Alleen Privacy en Security Officer heeft het recht om in te schrijven in en wijzigingen aan te brengen in de Verklaring van Toepasselijkheid.	Oudere versies van S.o.A.//V.v.T. worden bewaard voor een periode van 3 jaar.
Risicobehandelingsplan (elektronisch formulier – Word-document)	MS- Teams-omgeving, Kanaal: *In-formatie en beveiliging*	Privacy en Security Officer	Alleen Privacy en Security Officer heeft het recht om in te schrijven in en wijzigingen aan te brengen in het risicobehandelings- plan.	Oudere versies van risk treatment plan worden bewaard voor een periode van 3 jaar.

4. Validiteits- en documentbeheer

Dit document is geldig vanaf 01-01-2025. De eigenaar van dit document is de Privacy en Security Officer, die verplicht is om het minstens één keer per jaar te controleren en eventueel bij te werken voordat de bestaande risicobeoordeling op reguliere basis wordt herzien.

Bij het evalueren van de doeltreffendheid en geschiktheid van dit document moeten we rekening houden met de volgende criteria:

- Het aantal incidenten dat is voorgekomen maar niet in de risicobeoordeling is opgenomen.
- Het aantal risico's dat niet adequaat is behandeld.
- Het aantal fouten in het proces van risicobeoordeling en -behandeling als gevolg van onduidelijke definities van rollen en verantwoordelijkheden.