Strategie InformatieVeiligheid 2025-2029

Stichting Optimus Primair Onderwijs

Versieblad

Documenttitel	Strategie InformatieVeiligheid
Versie	0.99
Datum	18-03-2024
Status	Definitief
Classificatie	Openbaar
Proceseigenaar	A.Verwijst
Documentbeheerder	A.Verwijst

Wijzigingshistorie			

Goedkeuring		
Directievergadering	Datum	Agendapunt

Inleiding

Wij hechten veel waarde aan de beveiliging van informatie en privacy binnen onze organisatie. Dit document beschrijft onze strategie op het gebied van informatieveiligheid en privacy . We richten ons op het beschermen van waardevolle informatie en persoonsgegevens, wat essentieel is voor de continuïteit van ons onderwijsproces en het creëren van een veilige leer- en werkomgeving.

1.1 InformatieVeiligheid

InformatieVeiligheid staat voor beveiliging van waardevolle informatie (Security) en bescherming van persoonsgegevens (Privacy). Beschikbaarheid, Integriteit en Vertrouwelijkheid van de informatie zijn kernbegrippen. Bovendien is het belangrijk om veerkracht te integreren in onze beveiligingsstrategieën.

InformatieVeiligheid is binnen Optimus essentieel voor:

1. de continuïteit van het onderwijsproces;
2. kwalitatief hoogwaardig onderwijs;
3. een veilige leer- en werkomgeving.

InformatieVeiligheid is geen doel op zich maar is randvoorwaardelijk om uitvoering te kunnen geven aan de missie en koers van Stichting Optimus Primair Onderwijs.

1.2 Missie

Stichting Optimus Primair Onderwijs heeft als doel om kinderen een solide basis te geven en hen te helpen opgroeien tot gelukkige, zelfstandige en kritische wereldburgers. Gedurende hun gehele schoolloopbaan streven we ernaar dat kinderen zich erkend voelen in hun etnische en culturele achtergrond, evenals in hun geloof en levensovertuiging. Bovendien willen we het bewustzijn en de vaardigheden van kinderen versterken, zodat ze vanuit hun persoonlijke morele kompas in verbinding kunnen staan met anderen en kunnen bijdragen aan een duurzame samenleving en een kenniseconomie.

1.3 Uitgangspunten Koers

In de koers Optimus Wereldscholen 2022-2026 is de focus opgenomen voor de koersperiode. Deze focus is vertaald in de volgende uitgangspunten:

1. We blijven leren en zijn betrokken ambassadeurs;
2. We zijn bewust van kwaliteit en sturen daar gericht op;
3. We tillen het basisniveau omhoog;
4. We bieden leerlingen een breed fundament in hun ontwikkeling;
5. We bieden ieder kind gelijke kansen om te groeien;
6. We zijn een vitale duurzame organisatie;
7. We werken vanuit krachtige kennis.

Randvoorwaardelijk voor deze koers is een veilige en professionele leer- en werkomgeving, waarin de bescherming van informatie en persoonsgegevens centraal staat. Dit vereist een samenhangende aanpak van InformatieVeiligheid die voldoet aan de AVG-vereisten, om een voortdurend veilige en toekomstbestendige omgeving te waarborgen.

Strategie informatiebeveiliging en privacy

Onze strategie op het gebied van informatiebeveiliging en privacy is gerelateerd aan de drie aandachtsgebieden Governance, Processen en Technische Weerbaarheid. Deze aandachtsgebieden zijn essentieel voor het waarborgen van InformatieVeiligheid. Dit omvat de naleving van het IBP-AVG beleid, het garanderen van de veiligheid van de door de organisatie verstrekte informatie, en de verantwoordelijkheid nemen voor technische weerbaarheid.

De verantwoordelijkheden binnen de organisatie zijn als volgt

- Het College van Bestuur is eindverantwoordelijk en moet verantwoording kunnen afleggen aan de Raad van Toezicht.
- Alle leidinggevenden binnen Stichting Optimus Primair Onderwijs zien erop toe dat hun medewerkers voldoende geschoold zijn en het Informatiebeveiliging en Privacy beleid naleven.
- Iedere medewerker is verantwoordelijk voor de veiligheid van de informatie die door de organisatie beschikbaar wordt gesteld.
- Proceseigenaren zijn benoemd en zijn bewust van hun verantwoordelijkheid bij de uitvoer van processen waar informatieveiligheid een belangrijke rol speelt.
- IT is verantwoordelijk voor de technische weerbaarheid.

Governance rondom informatiebeveiliging en privacy

Alle te ondernemen acties in de processen en technische weerbaarheid zijn geborgd in de Governance. We weten wie wat doet met welk doel en in lijn met de strategische doelstellingen van de organisatie. De Governance rondom informatiebeveiliging en privacy gaat over het “wat en wie en met welk doel” en is gericht op de volgende thema’s:

1. Strategie: We sluiten aan bij de organisatiestrategie.
2. Beleid: We werken binnen vastgestelde kaders.
3. Architectuur: We werken vanuit een gekozen model.

4. Eigenaarschap: We benoemen rollen en verantwoordelijkheden en delen die toe.
5. Risk Management: We prioriteren op basis van een risicoanalyse.
6. Roadmap: We leggen de te nemen acties vast in de tijd en maken daar budget voor vrij.
7. Assurance: We laten ons toetsen.

Het belangrijkste doel van alle maatregelen is het mitigeren van de risico's die we lopen op het gebied van InformatieVeiligheid, waarmee we een veilige leer- en werk omgeving kunnen borgen. Assurance (goedkeuring) wordt echter een steeds belangrijker onderdeel van de Governance. Vanwege recente grote veiligheidsincidenten binnen het onderwijsveld neigt het Ministerie van Onderwijs steeds meer naar een verplichte externe audit waarbij externe verantwoording steeds belangrijker wordt.

1.4 IBP processen

Bij de volgende processen speelt InformatieVeiligheid een grote rol:

1. Human Resources: betreft borging expertise en training.
2. ITIL: betreft Incident, Problem, Change, en Configuration Management en Fysieke Beveiliging.
3. Datamanagement: betreft opslag, beheer, verwijderen (bewaartermijnen) en bescherming van gegevens.
4. Identity & Access Management (IAM): betreft toegangsregels en - rechten tot informatie.
5. Security Baselines: minimale afspraken over hoe veilig te werken
6. Business Continuity: betreft opvangen van incidenten (waaronder crisismanagement).
7. Cloud Leveranciers: goede afspraken en controle daarop bij externe leveranciers.

Aan ieder proces is een proceseigenaar toegewezen en de processen zijn beschreven.

1.5 Technische weerbaarheid

Bij technische weerbaarheid zijn de volgende thema's te onderscheiden:

1. Multi Factor Authenticatie/Thuiswerken: betreft veilig van buitenaf inloggen.
2. SOC SIEM: betreft 24 x 7 detectie van het netwerk (en respons).
3. Pentesten: betreft periodiek gericht testen op kwetsbaarheden in het netwerk.
4. Patchbeheer: betreft structureel bijwerken van de software (beveiligingsupdates).
5. Infrastructuur: betreft beschikbaarheid van het netwerk en systemen.
6. Security Policy: betreft inrichting technische beveiliging van het netwerk en systemen.
7. Computer Operations: betreft automatische IT-processen (bijvoorbeeld back-up).

Deze geïntegreerde benadering van InformatieVeiligheid is leidend voor alle activiteiten en maatregelen gericht op informatiebeveiliging en de bescherming van persoonsgegevens. We streven ernaar om als organisatie te groeien in volwassenheid op het gebied van InformatieVeiligheid, in lijn met de AVG-vereisten.

1.6 Slot en vervolg

Deze visie op en strategische uitgangspunten van InformatieVeiligheid zijn leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging en bescherming van de persoonsgegevens.

In het Informatiebeveiliging en privacy beleid zijn deze uitgangspunten uitgewerkt en gekaderd, zodat Stichting Optimus Primair Onderwijs planmatig kan groeien in volwassenheid en stappen zet in de richting waar ze als organisatie voor gaat.