G01 Strategie

Informatiebeveiliging en Privacy zijn geen op zichzelf staande onderwerpen. Ze dragen bij aan een veilige leer- en werkomgeving en sluiten daarmee aan op een groot aantal strategische uitgangspunten genoemd in het ‘Strategisch verhaal’ 2024 - 2028.

Onze organisatie werkt veel met waardevolle en vertrouwelijke informatie van jonge kinderen en medewerkers. De voortdurende ontwikkelingen op digitaal gebied maakt dat Informatiebeveiliging en Privacy een breed en complex onderwerp is geworden. Het werken vanuit een visie en strategische uitgangspunten voor Informatiebeveiliging en Privacy is daarom noodzakelijk om aantoonbaar te groeien naar een professionele en veilige manier van omgaan met de beschikbaar gestelde informatie.

Dit document geeft binnen de context van de door de RVKO benoemde strategische richting een basis om concreet en planmatig aan de slag te gaan met Informatiebeveiliging en Privacy.

Inhoud

1. Uitgangspunten

1.1 Informatiebeveiliging en Privacy

Informatiebeveiliging en Privacy staat voor beveiliging van waardevolle informatie (Security) en bescherming van persoonsgegevens (Privacy). De RVKO draagt hierin een grote verantwoordelijkheid.
Beschikbaarheid, Integriteit en Vertrouwelijkheid van de informatie zijn kernbegrippen.
Informatiebeveiliging en Privacy is essentieel voor:

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

Informatiebeveiliging en Privacy is geen doel op zich maar draagt bij aan de volgende strategische uitgangspunten van de RVKO:

1. toekomstbestendig onderwijs;
2. professionele (onderwijs)organisatie;
3. intrinsieke leer- en verbetercultuur;
4. een sterke organisatie.

1.2 Missie

De Rotterdamse Vereniging voor Katholiek Onderwijs biedt leerlingen hoogwaardig en eigentijds onderwijs, met hart en ziel. Dit doen we vanuit onze kernwaarden: verwondering, respect, verbondenheid, zorg, gerechtigheid, vertrouwen en hoop.

1.3 Visie in relatie tot Informatiebeveiliging en Privacy

De RVKO wil een veilige en professionele leer- en werkomgeving aanbieden en daarbij is het noodzakelijk dat de door de RVKO verzamelde, verwerkte en gepubliceerde informatie te allen tijde beschikbaar, correct en beschermd is. Dit vraagt om een strategisch samenhangende aanpak van Informatiebeveiliging en Privacy, die aantoonbaar aan de eisen voldoet, om blijvend een veilige en toekomstbestendige leer- en werkomgeving beschikbaar te stellen.

2. Strategie

Bij de RVKO hebben we een helder strategisch kader waarbinnen we sturen op autonomie in verbondenheid. Binnen onze organisatie hanteren we het subsidiariteitsbeginsel, waarbij het vertrouwen in de ander uitgangspunt is. Subsidiariteit houdt in dat de verantwoordelijkheid zo laag mogelijk in de organisatie wordt belegd. Dit betekent dat:

- mensen zich verantwoorden over de voortgang van de werkzaamheden en van de opbrengsten middels gesprekken en rapportages,
- we werken volgens het principe ‘pas toe of leg uit’,
- we onze scholen een hoge kwaliteit van ondersteunende diensten bieden vanuit het bestuursbureau,
- professionals, individueel en gezamenlijk, de ruimte krijgen om hun kwaliteiten en talenten in te zetten, om zo optimaal bij te kunnen dragen aan de doelen van de school en de RVKO.

Bron: RVKO Strategisch verhaal 2024 - 2028

2.1 Strategische uitgangspunten

Met betrekking tot Informatiebeveiliging en Privacy onderscheiden we 3 aandachtsgebieden:

1. Governance
2. Processen
3. Technische Weerbaarheid

Hiermee hebben we het volgende op het oog:

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

2.2 Governance

De Governance 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. Toetsing: We laten ons toetsen.

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.

Het belangrijkste doel van alle maatregelen is het mitigeren van de risico’s die we lopen op het gebied van Informatiebeveiliging en Privacy, waarmee we een veilige leer- en werk omgeving kunnen borgen. Certificering (goedkeuring) wordt echter een steeds belangrijker onderdeel van de Governance. Een Certificering kan alleen gegeven worden door een professionele externe auditor. Vanwege recente grote veiligheidsincidenten binnen het onderwijsveld wordt er ook voor het Funderend Onderwijs door het Ministerie van Onderwijs ingezet op een normenkader voor informatiebeveiliging en privacy. Verantwoording over het voldoen aan de vastgestelde minimale beveiligingseisen is hierbij van belang met de kanttekening dat een verplichte externe audit hiervan onderdeel kan gaan uitmaken.

2.3 IBP processen

Bij de volgende processen speelt Informatiebeveiliging en Privacy 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 (persoons)gegevens.
4. Identity & Access Management (IAM): betreft toegangsregels en toegangsrechten 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 op de afspraken met externe leveranciers.

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

2.4 Technische weerbaarheid

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

1. Multi Factor Authenticatie/Thuiswerken: betreft veilig van buiten de organisatie 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).

De bovenstaande thema's zullen uitgevoerd of onder regie uitbesteed worden door de IT-afdeling. Zij zullen hierover in begrijpelijke taal rapporteren aan het College van Bestuur. Bij deze rapportage hoort ook een financieel overzicht, zodat duidelijk is welke veiligheidsmaatregelen horen bij de gemaakt kosten/investeringen.
De thema's Multi Factor Authenticatie/Thuiswerken, SOC SIEM en Security Policy vallen onder het zogenaamde Zero Trust principe.

2.5 Slot en vervolg

Deze visie op en strategische uitgangspunten van Informatiebeveiliging en Privacy zijn leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging en bescherming van de persoonsgegevens. Hierbij zullen de genomen maatregelen zodanig worden afgewogen dat deze enerzijds aansluiten bij de belangen van de organisatie en anderzijds voldoen aan alle relevante wet- en regelgeving.
In het Informatiebeveiliging en privacy beleid zijn deze uitgangspunten uitgewerkt en gekaderd, zodat de RVKO planmatig kan groeien in volwassenheid en de juiste stappen zet in de richting waar ze als organisatie voor gaat.