Strategie Informatiebeveiliging en Privacy

Koning Willem I College

Inhoud

1. Missie, Visie en Strategische koers

Wij volgen de vastgestelde Missie, Visie en Strategische koers zoals beschreven in de onderstaande paragrafen.

1.1 Missie

KW1C is de spil in de regio voor het verbinden van onderwijs, werkveld en samenleving. Wij leiden studenten op tot vakbekwame professionals en versterken duurzaam de regio door een breed en toegankelijk onderwijsaanbod voor alle leeftijden, waarbij persoonlijke groei en maatschappelijke impact centraal staan.

1.2 Visie

In 2030 zijn we de meest toonaangevende en gewaardeerde mbo-instelling van Nederland op het gebied van onderwijskwaliteit, innovatie en inclusief onderwijs. We zijn een wendbare organisatie die in de regio is verankerd. Dichtbij de student, het werkveld en de samenleving, zodat we onderwijs aanbieden dat voor alle partijen relevant is.

1.3 Strategische koers

De strategische koers, “hoe gaan we onze visie en ambitie realiseren" is beschreven in de Routekaart.

Koning Willem I College werkt veel met waardevolle en vertrouwelijke informatie en met de voortdurende ontwikkelingen op digitaal gebied is Informatiebeveiliging en Privacy een breed en complex onderwerp 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 Koning Willem I College benoemde strategische richting een basis om concreet en planmatig aan de slag te gaan met Informatiebeveiliging en Privacy.

1.4 Informatiebeveiliging en Privacy

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

- De continuïteit van het onderwijsproces;
- Kwalitatief hoogwaardig onderwijs;
- Een veilige leer- en werkomgeving.

Informatiebeveiliging en Privacy is geen doel op zich maar draagt bij aan de volgende strategische uitgangspunten van Koning Willem I College:
- Toekomstbestendig onderwijs;
- Professionele (onderwijs)organisatie;
- Intrinsieke leer- en verbetercultuur;
- Een sterke organisatie.

1.5 Visie in relatie tot Informatiebeveiliging en Privacy
Koning Willem I College wil een veilige en professionele leer- en werkomgeving aanbieden en daarbij is het noodzakelijk dat de door Koning Willem I College 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

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 Koning Willem I College 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 werkomgeving 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 neigt het Ministerie van Onderwijs steeds meer naar een verplichte externe audit waarbij externe verantwoording steeds belangrijker wordt.

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 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 (ketenafhankelijkheid): goede afspraken en controle daarop bij externe leveranciers.

Aanvullende processen die niet benoemd worden binnen het NBA kader, maar wel worden meegenomen:
8. Studentenadministratie- en – registratie;
9. Digitale leeromgevingen;
10. Toetsen en examinering;
11. Personeelsadministratie;
12. Onderzoek data- en projecten;
13. Communicatie met ouders, studenten en medewerkers;
14. Toegang en gebruik van IT-faciliteiten;
15. Beheer van camera's en toegangscontrole;
16. Alumni netwerken en externe partners;
17. Incident- en klachtafhandeling.

Aan ieder proces is een proceseigenaar toegewezen en de processen zijn beschreven in de MORA[1].

2.4 Technische weerbaarheid
Bij technische weerbaarheid zijn o.a. de volgende thema's te onderscheiden:
1. Multi Factor Authenticatie/Thuiswerken: betreft veilig van buitenaf inloggen.
2. SOC SIEM[2]: 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 Informatievoorziening. 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.
In het Informatiebeveiliging en privacy beleid zijn deze uitgangspunten uitgewerkt en gekaderd, zodat Koning Willem I College planmatig kan groeien in volwassenheid en stappen zet in de richting waar ze als organisatie voor gaat.

[1] MORA: Mibbelbaar beroepsOnderwijs Referentie Architectuur
[2] SOC SIEM: Security Operations Center – Security Information and Event Management