Thomas More Hogeschool

G01 Strategie

Versiebeheer

Versie	Status	Datum	Omschrijving
0.1	Concept	11-2-2023	1e Draft
0.2	Concept	5-4-2023	Tekstuele aanpassingen
0.3	Concept	18-9-2023	Tekstuele aanpassingen
0.4	Concept	6-11-2023	Tekstuele aanpassing op verzoek CvB (voorbehoud goedkeuring)
1.01	Concept	11-10-2024	Tekstuele aanpassingen

Vastgesteld door Thomas More Hogeschool

Versie	Datum	Naam	Functie
1.0	24-10-2023	CvB	College van Bestuur
1.1	7-11-2024	CvB	College van Bestuur

INHOUDSOPGAVE

1. Inleiding

Informatiebeveiliging en Privacy is geen opzichzelfstaand onderwerp. Het draagt bij aan een veilige leer- en werkomgeving en sluit daarmee aan op een groot aantal strategische uitgangspunten genoemd in het Strategisch plan 2019-2024.

Onze organisatie werkt veel met waardevolle en vertrouwelijke informatie van studenten en medewerkers. De voortdurende ontwikkelingen op digitaal gebied maakt dat 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 Thomas More Hogeschool benoemde strategische richting een basis om concreet en planmatig aan de slag te gaan met Informatiebeveiliging en Privacy.

1.1 Informatiebeveiliging en Privacy

Informatiebeveiliging en Privacy staat voor beveiliging van waardevolle informatie (Security) en bescherming van persoonsgegevens (Privacy). Thomas More Hogeschool 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 Thomas More Hogeschool:

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

1.2 Missie

We zijn een onderwijsgemeenschap van studenten, opleiders, leraren, schoolleiders en onderzoekers. We willen er voor zorgen dat alle leerlingen in Rotterdam en regio wereldwijze en eigenzinnige onderwijsprofessionals ontmoeten, die geloof hebben in ieder kind en dit nooit opgeven, die er met hart & ziel willen zijn voor kinderen.

We bieden een oefenplaats om, door samen opleiden, onderzoeken en professionaliseren, bij te dragen aan een inclusieve samenleving die mens en natuur hoopvolle perspectieven biedt.

1.3 Visie in relatie tot Informatiebeveiliging en Privacy

Thomas More Hogeschool wil een veilige en professionele leer- en werkomgeving aanbieden en daarbij is het noodzakelijk dat de door de Thomas More Hogeschool 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

Uitgangspunt van onze kwaliteitscultuur is dat onderwijsprofessionals de drijfveer hebben om elke dag te realiseren wat ze van belang vinden in hun praktijk, dat ze kwaliteit willen leveren in het licht van de missie van onze onderwijsgemeenschap, dat hun expertise hen in staat stelt om dat te doen, dat ze zich professioneel willen ontwikkelen en bereid zijn zich te verantwoorden.

De komende jaren optimaliseren we de ruimte voor professionele ontwikkeling, door structuren en systemen die ontwikkeling belemmeren, weg te halen en te vervangen door nieuwe, meer passende structuren.

Bron: Thomas More Strategisch plan 2019 | 2024

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 Thomas More Hogeschool 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 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: goede afspraken en controle daarop bij externe leveranciers.

Aan ieder proces is een proceseigenaar toegewezen en de 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 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).

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 de bescherming van de persoonsgegevens van alle betrokkenen. 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.