Strategie Informatiebeveiliging en Privacy

HAS green academy

Versiebeheer

Versie	Status	Datum	Auteur	Omschrijving
0.1	Concept	21-11-2022	Leo Jaarsma, Ludo Cuijpers	1e Draft
0.2	Concept	20-12-2022	Leo Jaarsma, Ludo Cuijpers	Tekstuele aanpassingen
0.9	Concept	27-9-2023	Leo Jaarsma, Ludo Cuijpers	Aanpassing onderwijsvisie
0.91	Concept	25-3-2024	Leo Jaarsma, Ludo Cuijpers	Aanpassen titel op verzoek van Hans Camps en Martien van Gurp

Vastgesteld door HAS green academy

Versie	Datum	Naam	Functie
1.0	8-04-2024	Hans Camps	Lid College van Bestuur

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 HAS green academy Instellingsplan 2024-2027.
Onze organisatie 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 HAS green academy 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). HAS green academy 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 HAS green academy:

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

1.2. Missie

HAS green academy is dé kennisinstelling waar iedereen met hart voor het groene domein zich voortdurend kan ontwikkelen om optimaal bij te dragen aan een toekomst met genoeg gezond voedsel in een gezonde leefomgeving.

1.3. Visie in relatie tot Informatiebeveiliging en Privacy

De ontwikkelingen in de samenleving, het groene domein en het hoger onderwijs vragen om een hogeschool die zich blijft ontwikkelen tot kennisinstelling van de toekomst. Dat vertaalt zich in:

- ambitieuze onderwijsprogramma's voor studenten en professionals;
- toonaangevend onderzoek op een beperkt aantal zwaartepunten;
- maatwerk in de samenwerking met het werkveld;
- nieuwe stappen om inhoud te geven aan een Leven Lang Ontwikkelen;
- versterking van de internationale oriëntatie.

HAS green academy wil een veilige en professionele leer- en werkomgeving aanbieden en daarbij is het noodzakelijk dat de door HAS green academy 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. Cultuur en strategie

Cultuur: HAS green academy ziet zichzelf als een 'verbindende verkenner' met hart voor het groene domein en met als belangrijkste kernwaarden: Nieuwsgierig, Inclusief en Ondernemend. De HAS als organisatie en de mensen van de HAS zijn authentiek, aandachtig en ambitieus.

Strategie: De missie en toekomstvisie vertalen we in acht uitdagende ambities die we zowel HAS-breed als per cluster en afdeling gaan concretiseren en realiseren:

1. scherper keuzes maken op basis van onze missie;
2. bredere uitbouw van ons onderwijsportfolio;
3. versterking van onze onderzoekscultuur;
4. versteviging van de samenwerking met partners en werkveld;
5. versterking van banden met internationale partners;
6. wendbaarder maken van de organisatie;
7. verduurzaming van de eigen organisatie en gebouwen;
8. verbetering van onze positionering en zichtbaarheid.

Morgen en overmorgen: Bouwen op gemeenschappelijke grond. We vertrouwen erop dat we dit Instellingsplan kunnen vertalen in concrete stappen waarmee we onze missie waar kunnen maken: bijdragen aan een toekomst met genoeg gezond voedsel in een gezonde leefomgeving. We denken dat gezamenlijk te kunnen doen, ondanks de tendens tot polarisatie in de samenleving. HAS green academy koestert de verbinding en verdieping. Dat is waar jonge mensen baat bij hebben. [1]

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 HAS green academy 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.

[1] HAS GREEN ACADEMY INSTELLINGSPLAN 2024-2027, Definitieve versie 29 juni 2023, na instemming HR (15 juni) en RvT (22 juni).

6. Roadmap: We leggen de te nemen acties vast in de tijd, maken daar budget voor vrij en rapporteren daarover .
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.
Assurance (goedkeuring) wordt echter een steeds belangrijker onderdeel van de Governance. Een Assurance kan alleen gegeven worden door een Register Accountant (RA) of een Register EDP-Auditor (RE). 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 informatiebeveiliging en bescherming van de persoonsgegevens.

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