Beleid Informatiebeveiliging en Privacy

HAS green academy

Januari 2025, ‘s-Hertogenbosch

Hogeschool voor agro, food en leefomgeving


HAS green academy

Versies

Versiebeheer

Versie	Status	Datum	Auteur	Omschrijving
0.1	Concept	11-12-2022	Ludo Cuijpers	Bron Sebas van Tright
0.11	Concept	12-1-2023	Ludo Cuijpers Leo Jaarsma	Hoofdstuk 3 Governance is gewijzigd t.o.v. het huidige Beleid
0.12	Concept	16-1-2023	Ludo Cuijpers Leo Jaarsma Pieter van de Kerk	Diverse kleine aanpassingen
0.9	Concept	31-1-2024	Ludo Cuijpers Leo Jaarsma	Aanvullingen Liz Chermin verwerkt
0.91	Concept	3-4-2024	Ludo Cuijpers Leo Jaarsma	Naam gewijzigd. ROSA toegelicht in voetnoot. Bijlage 2 voorzien van inleiding. Evaluatie tweejaarlijks.

Vastgesteld door HAS green academy

Versie	Datum	Naam	Functie
1.0	8-4-2024	Hans Camps	Lid College van Bestuur


HAS green academy

1. Verantwoording en richtlijnen

1.1. Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan, met name ook van minderjarigen[1]. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

1.2. Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.
Informatiebeveiliging richt zich op de volgende aspecten:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten volledig, juist en actueel zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades, boetes en imagoverlies.

1.3. Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens[2].

1 Groene woorden worden in bijlage 1 (Verklarende woordenlijst) toegelicht

2 Bewerkt artikel 2, lid 2 van de AVG.

1.4. Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één geheel: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis op informatiebeveiliging en privacy binnen HAS green academy te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

1.5. Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en een bijdrage leveren aan de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen van wie HAS green academy persoonsgegevens verwerkt, waaronder studenten, samenwerkingspartners en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers en studenten) wordt gerespecteerd en HAS green academy voldoet aan relevante wet- en regelgeving.

1.6. Reikwijdte

- Het IBP-beleid binnen HAS green academy geldt voor alle betrokkenen, te weten: medewerkers, studenten, (geregistreerde) bezoekers en externe relaties (inhuur/ outsourcing).

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van HAS green academy. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken (b.v. uitspraken van medewerkers en studenten in discussies, op (persoonlijke pagina's van) websites en of social media.). Onder dit beleid[3] vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van HAS green academy evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

3 Dit beleid wordt nader uitgewerkt in een reglement.

IBP-beleid heeft binnen HAS green academy raakvlakken met:

- Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement (Integrale veiligheid), huisvesting en ongevallen.
- Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
- IT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen
- Medezeggenschap van studenten en medewerkers.

1.7. Concretisering

HAS green academy hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het **College van Bestuur** van HAS green academy neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.

2. HAS green academy voldoet aan alle **relevante wet- en regelgeving.**

3. Bij HAS green academy is de verwerking van persoonsgegevens altijd gekoppeld aan een **specifiek** doel en gebaseerd op één van de **wettelijke grondslagen**. Een goede balans tussen het belang van HAS green academy om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten allen tijde hun toestemming in- en herzien.

4. HAS green academy zal alle **betrokkenen helder en actief** informeren over de verwerkingen van hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, aanvullen, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit, afscherming en profilering van hun persoonsgegevens.

5. HAS green academy legt alle **verwerkingen van persoonsgegevens** vast in een dataregister (register van verwerkingen) en zal deze up-to-date houden. HAS green academy voldoet hiermee aan de documentatieplicht, zoals benoemd in de AVG.

6. Binnen HAS green academy is het **veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van eenieder.** Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.

7. HAS green academy is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het **eigendom** (auteursrecht) **toebehoort aan derden.** Medewerkers en studenten worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. HAS green academy **classificeert informatie en informatiesystemen.** De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.

9. HAS green academy (manager I&I) sluit met **alle leveranciers van digitale onderwijsmiddelen** (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken.

10. HAS green academy verwacht van alle **medewerkers, studenten, (geregistreerde) bezoekers en externe relaties dat zij**

zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. HAS green academy heeft hiervoor een privacy regelement (en privacy verklaring) geformuleerd, vastgesteld en geïmplementeerd.

11. **Informatiebeveiliging en privacy is bij HAS green academy een continu kwaliteitsproces,** waarbij regelmatig (minimaal tweejaarlijks) wordt geaudit of een self assessment wordt uitgevoerd en wordt gekeken of een aanpassing gewenst dan wel noodzakelijk is.

12. HAS green academy kijkt bij **wijzigingen** (denk ook aan uitfasering) in de infrastructuur of de **aanschaf van nieuwe (informatie) systemen** vóóraf naar de impact (middels DPIA) hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

13. HAS green academy neemt **passende organisatorische of technische (beveiligings)maatregelen** om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.

14. HAS green academy zal alle **beveiligingsincidenten en datalekken** vastleggen, volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

15. HAS green academy kiest ten aanzien van informatiebeveiliging **(autorisatie en authenticatie)** voor de vooronderstelling "Alles is in principe verboden tenzij het uitdrukkelijk is toegelaten"[4] in plaats van de zwakkere regel "Alles is in principe toegelaten tenzij het uitdrukkelijk is verboden".

4 Op basis van functie/rollen worden rechten door de leidinggevende toegekend. Een functioneel beheerder kent de rechten feitelijk toe. Bijvoorbeeld: een HR adviseur mag alleen de dossiers van de aan hem/haar toegewezen medewerkers inzien, als dat noodzakelijk is vanwege de opgedragen werkzaamheden.

2. Compliance

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

2.1. Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het Hoger onderwijs en wetenschappelijk onderzoek (WHW)
- Branche code Goed Bestuur Hogescholen – Vereniging Hogescholen
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- Archiefwet
- Auteurswet

Het NBA (Nederlandse Beroepsvereniging van Accountants) toetsingskader is leidend voor de te nemen beveiligingsmaatregelen. HAS green academy hanteert het Toetsingskader NBA en Privacy dat ontwikkeld is door SURF.

2.2. Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de vijf vuistregels met betrekking tot de omgang met persoonsgegevens te weten:

1. **Doelbepaling en doelbinding:** persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld, inclusief de bewaartermijnen. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag:** verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.
3. **Dataminimalisatie:** bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie:** de school legt aan betrokkenen (studenten en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast heeft de betrokkene recht op informatie, inzage, verbetering, aanvullen, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens ten behoeve van automatische profilering.
5. **Dataintegriteit:** er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens volledig, juist en actueel zijn.

2.3. Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in dataregisters.

2.4. Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd op basis van het ROSA[5] model. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitscriteria die van belang zijn.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden middels een centraal ingeregeld DPIA (Data Protection Impact Assessment). Vanaf de start van nieuwe (ICT)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

2.5. Beveiligingsincidenten en datalekken

Alle medewerkers die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken.
Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld bij privacy@HAS.nl.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden. Beveiligingsincidenten met een grote impact zullen terstond worden besproken en opgepakt. Studenten en externen kunnen kwetsbaarheden ook melden bij privacy@HAS.nl.

2.6. Planning en controle

Dit IBP-beleid wordt tweejaarlijks gereviewed en eventueel bijgesteld in opdracht van het bestuur. Het toezicht hierop berust bij de afdeling Finance & Control.
Hierbij wordt rekening gehouden met:

1. de status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
2. de actuele geinventariseerde risico's;
3. de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan.

---

5 De ROSA richt zich als ketenreferentiearchitectuur voor het onderwijsdomein op alle onderwijssectoren en op (onderwijs) sectoroverstijgende aspecten van informatievoorziening. Centraal staat de gegevensuitwisseling tussen functies/partijen en de invulling daarvan. Zie: https://ROSAWIKIXL.NL

Daarnaast kent HAS green academy een jaarlijkse verbeterplan voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het IBP-beleid wordt opgenomen in de PDCA cyclus van HAS green academy. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving etcetera meegenomen. Een en ander leidt tot een jaarlijkse Roadmap.

2.7. Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Naleving van ons IBP-beleid is een primaire verantwoordelijkheid van alle medewerkers binnen HAS green academy. Daarboven nemen de leidinggevenden en proceseigenaren hun verantwoordelijkheid om hun medewerkers aan te spreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, d.m.v. een instelling brede gedragscode, d.m.v. periodieke bewustwordingscampagnes, etcetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.
Mocht de naleving van dit beleid ernstig tekort schieten, dan kan HAS green academy de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

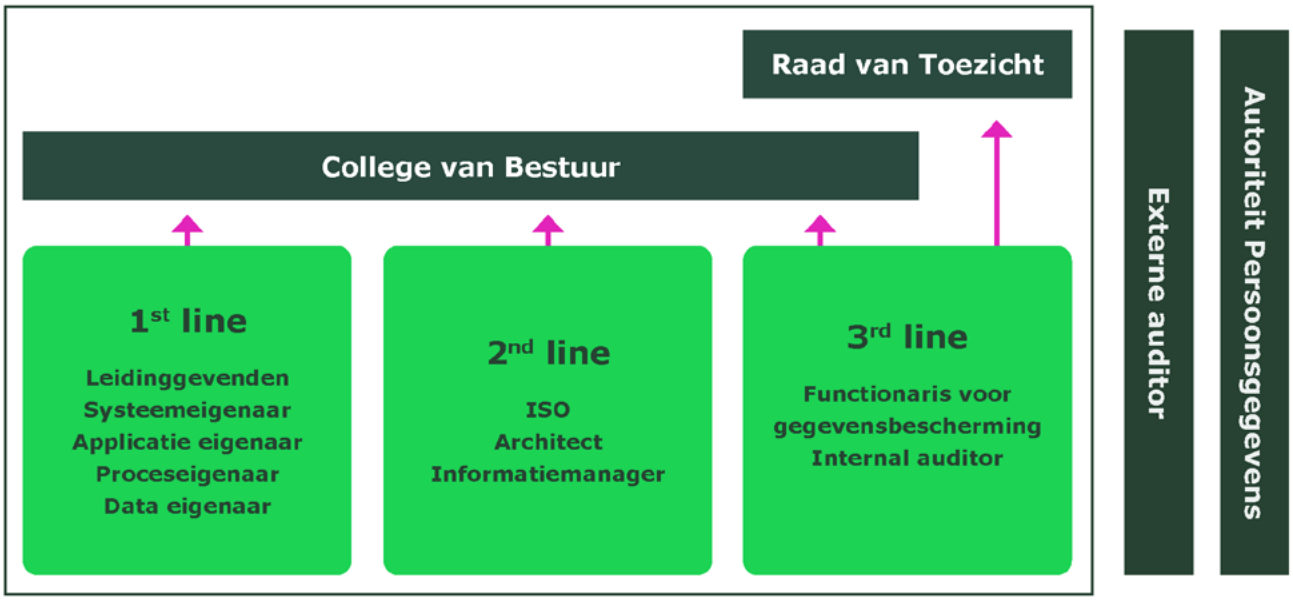
2.8. Logging en monitoring

Logging en monitoring door het team ICT zorgt er voor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk (zogenaamd SOC SIEM).

3. Governance

3.1. Rollen en verantwoordelijkheden

HAS green academy hanteert het three lines model. De eerste lijn binnen dit model is cruciaal, immers de leidinggevenden moeten er op toezien dat de AVG wordt nageleefd. Daartoe zijn alle managers geschoold en zij zien erop toe dat al hun teamleden handelen volgens het vastgesteld IBP beleid. Schematisch als volgt weergegeven.



Toelichting: De 1e, 2e en 3e line moeten afzonderlijk van elkaar (op verzoek) verantwoording afleggen aan het CvB.

3.2. De first line of defense: Leidinggevenden, Systeemeigenaar, Applicatie eigenaar, Proceseigenaren en Dataeigenaren

Leidinggevenden (Cruciale rol 1e lijn)

De eerste lijn is verantwoordelijk voor de volgende onderwerpen:

1. Scholing leidinggevende (1e lijn).
2. Scholing medewerkers (inclusief awareness).
3. Naleving afspraken (voorkomen schaduwadministraties).
4. Registreren toegekende extra autorisaties.
5. Toezien op verwerkersovereenkomsten van decentrale applicaties die gebruikt worden binnen hun organisatorische eenheid.

Systeemeigenaar

De systeemeigenaar is eigenaar van alle componenten in het ICT netwerk. Het functioneel beheer en de scholing van de medewerkers in de applicaties valt niet onder de verantwoording van de systeemeigenaar. Het functioneel beheer valt onder de applicatie-eigenaar van de desbetreffende applicatie. De systeemeigenaar faciliteert het technische proces, maar is niet verantwoordelijk voor de inhoud of het beheer van een applicatie.

Applicatie-eigenaar

De applicatie-eigenaar is de eigenaar van de desbetreffende applicatie die hem/haar is toegewezen. De applicatie-eigenaar is verantwoordelijk voor:

1. Inrichten van de applicatie conform de eisen van het IBP-beleid;
2. Vaststellen van een autorisatiematrix en een passende toegangsverleningsprocedure;
3. In samenspraak met de proceseigenaar vaststellen van de rollen en rechten van medewerkers;
4. Toezien op leveranciersmanagement, waaronder het jaarlijks beoordelen van de verwerkersovereenkomst en beveiligings-aspecten, ondersteund door de afdeling Inkoop;
5. Periodiek laten uitvoeren van een data protection impact assessment, indien dit noodzakelijk is conform wetgeving.

Proceseigenaren

De proceseigenaren[6] worden door het College van Bestuur benoemd. De proceseigenaar zal in overleg met de applicatie-eigenaren de processen laten inrichten, doorgaans met behulp van applicaties waarvan hij de func-tionaliteit mee heeft bepaald. De proceseigenaar is daardoor ook verantwoordelijk voor bijvoorbeeld de inrichting van het systeem op basis van de principes uit dit beleid. Dit betekent bijvoorbeeld concreet dat de proceseigenaar verantwoordelijk is voor het vaststellen van rollen en rechten en de toetsing op need-to-know en dataminimalisatie binnen zijn proces en de bijbehorende applicaties.
De processen zoals opgenomen in de MORA/HORA zijn leidend.

Data eigenaren

1e lijn is eigenaar van de data behalve de data die vermeld is in de dataregisters.

De functioneel beheerder (geen onderdeel van 1e lijn)

Bundelt de rechten in een systeem tot een systeemrol en volgt procedures conform het inrichting- of beheerdocument voor die applicatie. De rechten op functionaliteiten en specifieke data worden vastgelegd in de autorisatiematrix. Op verzoek van leiding-gevenden worden deze rollen aan specifieke medewerkers toegekend.
De functioneel beheerder van een applicatie zorgt voor actuele autorisatiematrix, waarin is opgenomen welke rollen en rechten er zijn binnen de desbetreffende applicatie.

6 Doorgaans is de applicatie eigenaar ook de proceseigenaar (HRM of financiën). Uitzondering is het Leerling informatie sys-teem / Studenten informatiesysteem of Management Informatiesysteem.

Periodieke controle
De leidinggevende is verantwoordelijk voor de uitgifte van rollen en rechten van haar medewerkers. De leidinggevende dient periodiek (eens per zes maanden) te controleren of de uitgegeven rollen/rechten nog actueel zijn, de systeemeigenaar faciliteert hiervoor een proces.

Rollen en invulling

Rol	Toewijzing	Invulling
Systeemeigenaar	Manager Informatisering & IT	Aanbesteding en kostenplaatseigenaar en contract-eigenaar van systemen (hardware en applicaties)
Applicatie eigenaar	Manager Onderwijs, Onderzoek en Kwaliteit Manager Personeelszaken & Organisatie Manager Finance & Control Manager Onderwijs, Onderzoek en Kwaliteit Manager Marketing & Communicatie	Osiris AFAS AFAS Office 365 (categorie 1) incl. notulen CRM
Proceseigenaar	Managers benoemd op basis van de MORA/HORA architectuur	

3.4. De second line of defense: Information Security Officer (ISO) en Architect en Informatiemanager

De ISO, al niet samen met de Architect en Informatiemanager, monitort de toepassing en naleving van het informatie-beveiligings- en privacybeleid, adviseert over informatiebeveiliging en privacybescherming en ondersteunt de leidinggevenden. De ISO ontwikkelt waar nodig beleid op het gebied van informatiebeveiliging en privacy, het College van Bestuur stelt dit voorgenomen beleid vast.
De ISO wordt hiërarchisch aangestuurd door de Manager Informatisering & IT. De ISO vormt de second line of defense als het gaat om de bescherming van persoonsgegevens.

3.5. De third line of defense: de Functionaris voor Gegevensbescherming en interne auditor

a) Functionaris voor gegevensbescherming

HAS green academy heeft een interne toezichthouder op de verwerking van persoonsgegevens aangesteld. Deze toezicht-houder wordt functionaris voor gegevensbescherming genoemd (hierna: "FG"). De FG zal door HAS green academy tijdig worden betrokken bij alle aangelegenheden waar persoonsgegevens bij komen kij-ken. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie bij HAS green academy. HAS green academy heeft de FG aangemeld bij de nationale toezichthoudende autoriteit, de zogenaamde Autoriteit Persoonsgegevens.
De taken van de FG houden in:

- Het informeren en adviseren van alle betrokken partijen over hun verplichtingen onder de AVG.
- Het toezien op de naleving van de AVG en andere relevante privacywetgeving.
- Het toezien op de naleving van dit privacybeleid door HAS green academy.
- Het toezien op een Privacy Impact Assessment.
- Het behandelen van klachten over de toepassing van het privacyreglement.
- Fungeren als eerste aanspreekpunt voor en samenwerken met de Autoriteit Persoonsgegevens.

b) de interne auditor
Externe controles worden uitgevoerd door onafhankelijke accountants. Deze worden voorbereid, gepland en geformuleerd door de interne auditor van HAS green academy.

3.6. Implementatie beleid

Het College van Bestuur van HAS green academy is verantwoordelijk voor verwerkingen van persoonsgegevens waarvoor het doel en de middelen vaststelt. Het wordt aangemerkt als de verwerkingsverantwoordelijke in de zin van de wet AVG. De verantwoordelijkheid houdt kort samengevat in:

- Dat de persoonsgegevens verwerkt worden in overeenstemming met de vastgestelde doelen van de verwerking, dat die doelen gerechtvaardigd zijn en dat de verwerking zorgvuldig gebeurt.
- Dat hierover verantwoording kan worden afgelegd aan de Autoriteit Persoonsgegevens.

De feitelijke verwerking van persoonsgegevens wordt echter op allerlei lagen van HAS green academy uitgevoerd. Het is niet één cluster of dienst die effectief verantwoordelijk kan zijn voor alle persoonsgegevens die HAS green academy verwerkt. Er is een onderscheid tussen centrale verwerkingen, waarvoor de diensten ver-antwoordelijk zijn, en -aanvullend daarop- decentrale verwerkingen, waarvoor de clusters of individuele diensten zelf verantwoordelijk zijn.

3.7. Inpassing in de instellingsgovernance en afstemming met aanpalende beleidsterreinen

Om de samenhang in de organisatie met betrekking tot gegevensbescherming goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van verwerking van persoonsgegevens binnen de verschil-lende onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp privacy op verschillende niveaus.
Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacyaspecten. Het strategisch niveau wordt ingevuld door de leidinggevenden uit onderwijs en bedrijfsvoering (Information Board).
Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. Het tactisch niveau wordt ingevuld door de ISO.
Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan. Het operationeel niveau wordt ingevuld door de 1e lijn (leidinggevenden) bestaande uit: clusterdirecteuren, manager Onderwijs, Onderzoek en Kwaliteit, manager Personeelszaken & Organisatie, manager Finance & Control en manager Marketing & Communicatie, zowel op centraal als decentraal niveau.

3.8. Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Noodzakelijk is het om het bewustzijn voortdurend aan te scherpen, zodat bij HAS green academy kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende scholingen voor medewerkers en bewustwordingscampagnes voor medewerkers, studenten en relaties. Deze campagnes sluiten bij voorkeur aan bij landelijke campagnes in het mbo/hoger onderwijs, zo mogelijk in afstemming met andere of integrale beveiligingscampagnes. Verhoging van het bewustzijn is de verantwoordelijkheid van elke leidinggevende en wordt gefaciliteerd door de ISO.

3.9. Controle en naleving

Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert gezamenlijk met de ISO en de interne auditor de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens.
Eventuele externe controles worden uitgevoerd door onafhankelijke accountants. Deze externe controles worden gepland en geformuleerd in een nauwe samenspraak met de interne auditor van HAS green academy, al dan niet mede gefinancierd en georganiseerd door SURF.

Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten HAS green academy maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het beleid.

Bijlage 1: Verklarende woordenlijst

AVG:
Algemene Verordening Gegevensbescherming.

Beleid:
Beleid met betrekking tot het verwerken van persoonsgegevens door HAS green academy.

Betrokkene:
Een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft.

Broneigenaar:
Aangewezen directeur die verantwoordelijk is voor persoonsgegevens van één of meerdere categorieën van Betrokkenen. De Broneigenaar voert de persoonsgegevens in en zorgt voor de vernietiging. In de tussentijd leent hij ze uit aan de organisatorische eenheden binnen HAS green academy. De organisatorische eenheden mogen dan de persoonsgegevens verrijken.

Datalek:
Een inbreuk in verband met persoonsgegevens, die leidt tot enige ongeoorloofde verwerking daarvan. Hier vallen zowel opzettelijke als onopzettelijke inbreuken onder.

Dataportabiliteit:
Het recht om persoonsgegevens en informatie over te dragen aan een nieuwe verwerker zonder technische problemen.

Dataregister:
De AVG spreekt van het Register van Verwerkingsactiviteiten, dit is een overzicht van de persoonsgegevens die verwerkt worden, met informatie over het doel daarvan, de grondslag daarvoor, de bewaartermijnen van de gegevens en bron of ontvanger van de gegevens. HAS green academy heeft drie centrale registers: dat voor studentgegevens, voor medewerker gegevens en voor relatiegegevens. Het dataregister is het Register van Verwerkingsactiviteiten aangevuld met de BIV-classificatie en de autorisatie matrix op hoofdlijnen.

DPIA:
Data Protection Impact Assessment (Gegevensbeschermingseffectbeoordeling): een beoordeling die helpt bij het identificeren van privacy risico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau. Soms ook wordt de term PIA gebruikt, Privacy Impact Assessment.

Functionaris voor Gegevensbescherming:
Interne toezichthouder en privacy adviseur aangesteld door het College van Bestuur, op grond van artikel 37 van de AVG, ook wel aangeduid als FG

Minderjarige:
Voor de AVG geldt iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt. Buiten de AVG geldt uiter aard jonger als 18 jaar.

Niet-geautomatiseerde verwerking:
Voorbeelden: aangetekende stukken, pasjes die zichtbaar gedragen worden, klassenlijsten met foto's (smoelenboek), etc.

Persoonsgegeven:
Elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon.

Privacy by Default:
Een gegevensverwerking waarbij de standaardinstellingen van producten en diensten zo zijn ingesteld dat de privacy van betrokkenen maximaal wordt gewaarborgd. Dit betekent onder meer dat er zo min mogelijk gegevens worden gevraagd en verwerkt.

Privacy by Design:
Al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) wordt ten eerste aandacht besteed aan privacy verhogende maatregelen. Ten tweede wordt rekening gehouden met dataminimalisatie: er worden zo min mogelijk persoonsgegevens verwerkt, alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.

Verwerker:
Een door HAS green academy ingeschakelde (derde) partij die ten behoeve van HAS green academy, en op basis van haar schriftelijke instructies, persoonsgegevens verwerkt, e.e.a. vastgelegd in een verwerkersovereenkomst.

Verwerking:
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, afschermen, wissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke:
College van Bestuur van HAS green academy dat het doel en de middelen van de verwerking van persoonsgegevens vaststelt.

Bijlage 2: Gehanteerde referentie-documenten

Dit beleid wordt verder uitgewerkt in de volgende documenten:

Referentiedocumenten Governance:
NBADOC G01-Strategie
NBADOC G01-Strategie Audit
Voor HAS green academy is Informatiebeveiliging en Privacy essentieel voor de continuïteit, kwaliteit en veiligheid van het onderwijs. Dit sluit aan bij de volgende strategische uitgangspunten: toekomstbestendig onderwijs; professionele (onderwijs)organisatie; intrinsieke leer- en verbetercultuur en een sterke organisatie.
HAS green academy biedt een veilige en professionele leer- en werkomgeving aan. Daarbij zijn de door HAS green academy verzamelde, verwerkte en gepubliceerde informatie te allen tijde beschikbaar, correct en beschermd. 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.

NBADOC G02-Beleid
NBADOC G02-Beleid Audit
Door het College van Bestuur is een nieuwe versie van het Informatiebeveiliging en privacy beleid vastgesteld. Er is geen nieuwe versie gemaakt, alleen bijlage 2 is toegevoegd. Of de beschrijving van rollen en verantwoordelijkheden aansluit bij de situatie binnen HAS green academy zal moeten worden geëvalueerd. Tevens zal op termijn meer verwezen moeten gaan worden naar andere beleidstukken die bij de implementatie van het NBA-model vastgesteld zullen gaan worden.

NBADOC G03-Architectuur
NBADOC G03-Architectuur Audit
Werken vanuit een vastgesteld architectuur geeft duidelijkheid over waar welke informatie verwerkt wordt. Inzicht in het applicatielandschap en procesmatig werken zijn noodzakelijk om Informatiebeveiliging en Privacy te kunnen borgen in de hele organisatie. HAS green academy heeft het architectuurmodel HORA formeel vastgesteld als uitgangspunt voor de processen die we binnen onze organisatie hanteren. In het referentiedocument worden de statements van het NBA-model geplot op de HORA. Niet alle statements komen voor in het HORA-model, maar het is de bedoeling dat ze daarin wel opgenomen worden, evenals de BIV-classificatie van elk proces.

NBADOC G04-Eigenaarschap
NBADOC G04-Eigenaarschap Audit
Het benoemen eigenaarschap met betrekking tot Informatiebeveiliging en Privacy is essentieel om Informatiebeveiliging en Privacy te borgen in heel de organisatie. Duidelijk is dat het College van Bestuur de eindverantwoordelijkheid draagt. Ook dragen we uit dat iedereen een verantwoordelijkheid heeft om veilig om te gaan met de informatie die ons is toevertrouwd. Voor het adresseren van eigenaarschap gebruikt HAS green academy het RACI-model. Hierin zijn de verschillende verantwoordelijkheden met betrekking tot de thema's ondergebracht.
De eigenaren (accountable) zijn benoemd. De uitvoerders (responsible) zijn deels benoemd en moeten in sommige gevallen nog worden aangewezen. Wie verder nog betrokken moeten worden (consulted/informed) zal bij de uitvoering van de taken die genoemd zijn in de Roadmap verder worden ingevuld. Hierin zullen de Accountables begeleid en getraind worden door de Information Security Officer met als doel concreet te gaan werken vanuit de vastgestelde Governance.

NBADOC G05-Risk Management
NBADOC G05-Risk Management Audit
HAS green academy volgt de risicoanalyse die gemaakt is vanuit het SURF Cyberdreigingsbeeld. Op basis daarvan zijn de volgende risico's benoemd:
R1: Governance niet op orde
R2: Aanval Ransomware
R3: Afhankelijkheid van Cloud Computing
R4: Identiteitsfraude
R5: Niet hanteren van Bewaartermijnen
Het risicoactieplan van HAS green academy richt zich op de in het NBA genoemde beheersmaatregelen van bovengenoemde risico's. In de Roadmap zijn deze acties gekoppeld aan tijdlijn en eigenaar.

NBADOC G06-Roadmap
NBADOC G06-Roadmap Audit
De Roadmap geeft het groeipad aan dat HAS green academy moet doorlopen om de genoemde risico's te mitigeren. Deze risico-gebaseerde aanpak prioriteert de beheersmaatregelen die in het NBA-model staan. Voor alle onderwijssectoren (PO, VO, mbo, HO en Uni) is volwassenheidsniveau 3 (opzet en bestaan) voor de meeste NBA-statements het gewenste niveau. HAS green academy onderschrijft dit en meent zelfs dat voor een groot aantal statements volwassenheidsniveau 4 haalbaar (en gewenst) is als de beheersmaatregelen goed geborgd worden in de manier van werken. Sturen op een reëel en een risico gebaseerd actieplan is hierin effectiever dan werken met een compleet uitgewerkte Roadmap.

NBADOC G07-Toetsing
NBADOC G07-Toetsing Audit
Sluitstuk van de Governance is de onafhankelijke toetsing. HAS green academy ziet dit niet als een (eind)exa-men maar vooral als instrument om de Informatiebeveiliging en Privacy op niveau te krijgen en houden. HAS green academy toetst (intern) en laat zich toetsen (extern).
Intern toetst de HAS green academy middels mini-assessments en DPIA's. Deze zijn opgenomen in de Roadmap. Een uitgebreidere interne audit wordt gedaan door de interne IT-auditor. Deze audit dient niet alleen om het College van Bestuur inzage geven over hoe de HAS green academy ervoor staat, maar ook als opmaat voor de externe toetsing en input voor de mbo Benchmark (hoe staan we er voor t.o.v. de andere onderwijsinstellingen).

Referentiedocumenten Processen:
NBADOC P08-Human Resources
NBADOC P08-Human Resources Audit
Betreft borging expertise en training.

NBADOC P09-ITIL
NBADOC P09-ITIL Audit
Betreft Incident, Problem, Change, en Configuration Management en Fysieke Beveiliging.

NBADOC P10-Data Management
NBADOC P10-Data Management Audit
Betreft opslag, beheer, verwijderen (bewaartermijnen) en bescherming van gegevens.

NBADOC P11-IAM
NBADOC P11-IAM Audit
Betreft toegangsregels en - rechten tot informatie.

NBADOC P12-Security Baselines
NBADOC P12-Security Baselines Audit
Minimale afspraken over hoe veilig te werken.

NBADOC P13-Business Continuity
NBADOC P13-Business Continuity Audit
Betreft opvangen van incidenten (waaronder crisismanagement).
NBADOC P14-Cloud Leveranciers (Ketenafhankelijkheid)
NBADOC P14-Cloud Leveranciers Audit
Goede afspraken en controle daarop bij externe leveranciers.

Referentiedocumenten Technische Weerbaarheid:
NBADOC T15-T21 Technische Weerbaarheid
NBADOC T15-T21 Technische Weerbaarheid Audit

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 gemaakte kosten/investeringen.
De thema's Multi Factor Authenticatie/Thuiswerken, SOC SIEM en Security Policy vallen onder het zogenaamde Zero Trust principe.


HAS green academy