Informatiebeveiligingsbeleid Avans Hogeschool

Herziening 2024

Vaststelling

Dit beleid is vastgesteld door het CvB van Avans Hogeschool en treedt in werking per 9 april 2024. Het beleid geldt totdat het wordt herzien dan wel ingetrokken.

De richtlijnen zijn niet vrijblijvend. Afwijking van de richtlijnen is alleen acceptabel op basis van een zorgvuldige risicoafweging. Deze afweging is altijd een besluit van de directie.

CISO

09-4-2024

Versiebeheer

Datum	Versie	Door	Wijziging
25-01-2023	0.5	J.J. vd Neut	Initiële versie
8-05-2023	0.8	J.J. vd Neut	1e ronde feedback verwerkt
13-06-2023	0.85	J.J. vd Neut	1e deel 2e feedbackronde verwerkt
16-06-2023	0.9	J.J. vd Neut	Concept voor advies Cirkel
01-09-2023	0.95	J.J. vd Neut	Definitief na verwerking opmerkingen Cirkel
15-12-2023	1.0	J.J. vd Neut	Aanpassingen ivm nieuwe structuur Privacy & Security governance, na overleg met nieuwe CISO
15-01-2024	1.01	Thijs Willems	Kleine tekstuele aanpassingen
09-02-2024	1.02	Thijs Willems	Aanpassingen nav review BE&C
04-03-2024	1.03	Arie Taal	Aanpassingen nav review Juridische Zaken

Samenvatting

Het succes van een organisatie hangt steeds meer af van informatie, nieuwe technologieën en computersystemen. Die informatie moet goed worden beveiligd, zeker als er persoonsgegevens worden opgeslagen. In dit document is verwoord op welke manier Avans Hogeschool voorziet in adequate informatiebeveiliging en daarmee voldoet aan relevante wet- en regelgeving.
Met het informatiebeveiligingsbeleid wil Avans Hogeschool ook bijdragen aan een betere kwaliteit van de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit, veiligheid en privacy.

Beschreven wordt op wie, op welke onderdelen van Avans Hogeschool en op welke apparaten en applicaties het beleid van toepassing is. Informatiebeveiliging werkt door in alle lagen van de organisatie. Naast de reikwijdte van het beleid worden de verantwoordelijkheden van de betrokken functionarissen beschreven. Het lijnmanagement is verantwoordelijk voor haar eigen processen, de directie zorgt ervoor dat beveiligingsmaatregelen daadwerkelijk worden geïmplementeerd. Eindverantwoordelijkheid voor informatiebeveiliging en de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen Avans Hogeschool ligt bij het College van Bestuur (CvB).

Vijf beleidsprincipes zijn leidend, namelijk:

1. *Risico-gebaseerd*
   We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.
2. *Iedereen*
   Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.
3. *Altijd*
   Informatiebeveiliging zit in het DNA van al onze werkzaamheden.
4. *Security by Design*
   Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.
5. *Security by Default*
   Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.

In het Privacybeleid is tevens het principe privacy-by-design beschreven.

beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert de grootste risico's. Bij Avans Hogeschool werken we daarom voortdurend aan het vergroten van het beveiligingsbewustzijn van medewerkers om kennis van risico's te verhogen en veilig en verantwoord gedrag aan te moedigen.

Informatiebeveiliging is een continu proces, waarbij we steeds kijken naar mogelijke verbeteringen. Dit gebeurt onder andere door jaarplannen, controles en bijsturing.

Inhoudsopgave

Inleiding

Het succes van Avans Hogeschool hangt steeds meer af van informatie, nieuwe technologieën en computersystemen. Avans Hogeschool richt zich op een geïntegreerde digitale leer-, werk- en onderzoeksomgeving. Door het gebruik van data kan het leerproces van de student effectiever en efficiënter worden ingericht. We kunnen niet meer zonder het digitaal verzamelen, vastleggen en delen van informatie met zowel interne als externe partners, collega's en studenten. Dit is met zoveel woorden ook beschreven in de Ambitie 2025 waarin voor het thema Tech & Data duidelijk staat dat de diensten aan moeten sluiten bij de behoeften van studenten, medewerkers en praktijkpartners.

De digitale werkelijkheid is constant in beweging en dat brengt steeds nieuwe en andere risico's met zich mee voor de veiligheid van informatie. De risico's vormen een bedreiging voor de kwaliteit en continuïteit van processen en voor het behalen van de strategische doelen. De bedreigingen kunnen de beschikbaarheid, integriteit en vertrouwelijkheid van informatie beïnvloeden. Voorbeelden van bedreigingen zijn kwetsbaarheden in systemen of ongeautoriseerde toegang tot informatie. Dit kan de waarde van een Avans Hogeschool-diploma(certificaat), behaalde cijfers of de legitimiteit van onderzoekconclusies ondermijnen. Ook de privacy[1] van o.a. studenten, medewerkers en gasten en de reputatie van Avans Hogeschool kunnen worden geschaad. Informatiebeveiliging is daarom van cruciaal belang.

Informatiebeveiliging vraagt steeds om bijstelling zodat er een passend beveiligingsniveau blijft. Dat komt onder andere door de technologische ontwikkelingen, de aangescherpte eisen om te voldoen aan de wet- en regelgeving rondom gegevensbescherming en privacy (AVG), en de afspraken met onderzoek- en onderwijspartners.

Het verkleinen en beheersen van de risico's vraagt om inspanningen op organisatorisch, procesmatig en technologisch vlak. Daarnaast moeten bestuurders, medewerkers, studenten en gasten van Avans Hogeschool zich ook bewust worden van de risico's en hun handelen daarop afstemmen.

De veiligheid van informatie is niet te bereiken door eenmalig technische en organisatorische maatregelen vast te stellen. Door de veranderende wereld is het een dynamisch proces. Het informatiebeveiligingsbeleid groeit mee met de ambitie van Avans Hogeschool, zoals onderstaand is weergegeven. Evenals het continu ontwikkelen binnen die ambitie moet het informatiebeveiligingsbeleid mee ontwikkelen met de organisatie die wendbaar en veerkrachtig is en digitaal transformeert. Geïntegreerde leer-, werk- en onderzoeksomgevingen brengen kansen maar ook risico's mee die door informatiebeveiligingsmaatregelen waar nodig gemitigeerd moeten worden.

Er is een belangrijke relatie tussen informatiebeveiligingsrisico's en risico's op andere gebieden, zoals privacy, safety[2] (arbowetgeving), veiligheid in onderwijs en onderzoek, fysieke beveiliging en business-continuïteit. Soms overlappen deze risico's elkaar gedeeltelijk. In bijlage A is een toelichting beschreven op de relatie tussen informatiebeveiliging en privacy. Onderhavig beleidsstuk richt zich primair op informatiebeveiliging.

[1] Voor het specifieke Privacy beleid van Avans Hogeschool zie <URL>
[2] *Safety* wordt als verzamelterm gebruikt voor de verschillende aspecten van personele veiligheid: Arbo en milieu, sociale veiligheid, bedrijfshulpverlening e.d.

Wet- en regelgeving
Avans Hogeschool wil in al haar processen en procedures voldoen aan relevante wet- en regelgeving. Waar de wet- en regelgeving ruimte biedt voor keuzes om op basis van risico-afwegingen mogelijk af te wijken, zullen we vanuit een risicomijdende houding kiezen voor voldoen-aan. Dit doen wij op basis van het principe “Pas toe of leg uit”, waardoor Avans Hogeschool altijd kan verantwoorden waarom zij op onderdelen niet voldoet. Afwijken vindt plaats op basis van een risicoafweging en acceptatie door het College van Bestuur. In bijlage B is een overzicht opgenomen van de relevante wet- en regelgeving.

De CISO zal ten minste iedere drie jaar in samenwerking met juridisch deskundigen van Avans Hogeschool of van derden, en relevante proces- en systeemeigenaren, een doorlichting doen van alle mogelijk relevante oude, nieuwe en aanstaande wet- en regelgeving. Hiermee zal het overzicht als in bijlage B worden bijgewerkt. Wijzigingen in de informatiebeveiliging ten gevolge van toepasselijke wijzigingen in wet- en regelgeving zullen worden verwerkt de relevante beleidsdocumenten, standaarden en processen.

Definitie, doelstelling, doelgroep en reikwijdte

Informatiebeveiliging

Informatiebeveiliging omvat het geheel van preventieve, detectieve, repressieve en correctieve maatregelen, beleid en procedures die worden ingezet om informatie te beschermen tegen niet-geautoriseerde toegang, wijziging, openbaarmaking, verlies, verstoring of vernietiging. Dit omvat zowel de fysieke als digitale beveiliging van data.

Doelstelling, randvoorwaarden en uitgangspunten

Informatiebeveiliging heeft de volgende doelen:

- Het waarborgen van de beschikbaarheid van informatie van het onderwijs, onderzoek en de bedrijfsvoering.
- Het waarborgen dat informatie juist, volledig en actueel is (integriteit) en alleen toegankelijk is voor personen die vanuit hun rol/functie daar toegang tot mogen hebben (beschikbaarheid, integriteit en vertrouwelijkheid).
- Het voorkomen van beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan beperken.

Met het informatiebeveiligingsbeleid wil Avans Hogeschool bijdragen aan een passende beveiliging binnen de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit, veiligheid en privacy en uiteraard de daarmee samenhangende kosten. Het Informatiebeveiligingsbeleid sluit daarmee aan bij de missie van Avans Hogeschool, “Bij Avans leiden we professionals op die klaar zijn voor de wereld van morgen”.

Avans Hogeschool heeft de ambitie om met behulp van dit beleidsdocument de informatiebeveiliging structureel naar volwassenheidsniveau 3 ‘Gedefinieerd[3]’van het SURF IB HO Toetsingskader te brengen en daar te houden. Dit doet zij door het beschrijven van verantwoordelijkheden, taken en bevoegdheden, continue verbetering en door te voldoen aan wet- en regelgeving.

Een belangrijk gegeven is de keuze van Avans Hogeschool voor in-house software development middels een Agile-benadering. Beide elementen zijn momenteel volop in ontwikkeling. De SURF-kaders kennen voornamelijk een ITIL-aanpak als basis. De combinatie van de genoemde onderdelen maakt dat Avans Hogeschool een forse inspanning voor zich ziet om informatiebeveiliging in te bedden in de Avans way-of-working. Het erkennen van deze tegenstelling vormt de basis voor een succesvol leertraject dat Avans Hogeschool met betrekking tot informatiebeveiliging moet doorlopen.

Avans Hogeschool gebruikt het Informatiebeveiligingsbeleid om op de IB-doelstellingen te sturen. Het Informatiebeveiligingsbeleid, en de opvolging daarvan, moet Avans Hogeschool in staat stellen ‘in control’ en compliant te zijn. Op basis daarvan kunnen de betrokken directeuren verantwoording afleggen aan het CvB, dat vervolgens verantwoording aflegt aan de Raad van Toezicht (RvT). De uitvoering van het beleid is ook de basis is om te voldoen aan wettelijke voorschriften.

[3] Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst. Zie meer op https://www.nba.nl/globalassets/over-de-nba/ledengroepen/lio/lio-new/nba-lio-norea-handreiking-bij-volwassenheidsmodel-informatiebeveiliging-januari-2019.pdf

Randvoorwaarden

Om de doelstellingen omtrent informatiebeveiliging te kunnen bereiken, zijn de volgende randvoorwaarden voor Avans Hogeschool van belang:

- *Beveiligingsorganisatie*
  De verantwoordelijkheden, taken en bevoegdheden van de informatiebeveiligingsfunctie zijn expliciet vastgelegd en worden gedragen door het bestuur, en afgeleid daarvan, door de hele instelling.
- *Procesbenadering*
  Informatiebeveiliging is een continu proces. Periodiek worden er risicoanalyses en audits uitgevoerd. De resultaten hiervan worden opgenomen in vastgestelde jaarplannen met duidelijke keuzes in beveiligingsmaatregelen. De uitvoering van deze beveiligingsmaatregelen wordt periodiek gecontroleerd.
- ITIL versus Agile werkwijze
  De inbedding van informatiebeveiliging volgens de SURF-benadering in de Agile Avans way-of-working, vereist het doorlopen van een indringend leertraject. Avans Hogeschool biedt de ruimte om dit leertraject te doorlopen en zodoende een stevig fundament voor informatiebeveiliging te realiseren.

Uitgangspunten

Uit de doelstellingen en de voornoemde randvoorwaarden komen de volgende uitgangspunten voort:

<u>Omgang Avans Hogeschool met dit beleid</u>

- *Strategisch beleid is kaderstellend*
  Dit informatiebeveiligingsbeleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan de vastgestelde beveiligingsprincipes, best practices en normen.
- *Normenkader en compliance*
  Specifiek voor de SURF gemeenschap[4] is het 'SURF Normenkader Informatie Beveiliging Hoger Onderwijs' (IBHO) vastgesteld. Het IBHO is gebaseerd op de normen die zijn vastgelegd in de ISO-27000-serie. Het IBHO vormt samen met onderhavig beleidsdocument de basis voor een informatie-beveiligingsmanagementsysteem van Avans Hogeschool. Het ISMS is ingericht op basis van de internationale standaard ISO 27001.
- *Volwassenheid*
  IBHO omschrijft een norm voor de volwassenheid van de Informatiebeveiliging volgens het Capability Maturity Model (CMM)[5]. Avans Hogeschool streeft uiteindelijk naar volwassenheidsniveau 3 'Gedefinieerd'[6] volgens de SURF-richtlijnen.
- *Maatregelen*
  Avans Hogeschool neemt maatregelen op basis van de internationaal vastgestelde ISO-27002-standaard. Hierbij worden de 'SURF Baseline Informatie Beveiliging Hoger Onderwijs' en overige best practices in de SURF-gemeenschap als uitgangspunt genomen. De specifieke maatregelen voor Avans Hogeschool zijn beschreven in de Governance Risk & Compliance applicatie Trustbound.

<u>Beveiligingsprincipes</u>

- *Risico-gebaseerd*
  Informatiebeveiliging is risico-gebaseerd. De maatregelen zijn gebaseerd op de mogelijke veiligheidsrisico's van informatie, processen en IT-faciliteiten van Avans Hogeschool.

---

[4] De actuele documenten zijn te vinden op https://www.surf.nl/informatiebeveiliging en https://www.surf.nl/surfaudit-inzicht-in-je-informatiebeveiliging-en-privacy en voor SCIPR-leden op de ondersteunende wiki's https://wiki.surfnet.nl/display/SCIPR/SCIPR+Home en https://wiki.surfnet.nl/display/SA/SURFaudit+Home

[5] https://nl.wikipedia.org/wiki/Capability_Maturity_Model

[6] Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst. Zie meer op https://www.nba.nl/globalassets/over-de-nba/ledengroepen/lio/lio-new/nba-lio-norea-handreiking-bij-volwassenheidsmodel-informatiebeveiliging-januari-2019.pdf

- *Iedereen*
  Informatiebeveiliging is een verantwoordelijkheid van iedereen, waarbij de diepgang in inhoud varieert met ieders individuele rol binnen Avans Hogeschool. Het strategisch informatiebeveiligingsbeleid en ook de daarbij horende beleidsstukken geven daarbij richting aan de van een individu in zijn/haar rol verwachte inzet.
- *Altijd*
  Informatiebeveiliging is een continu proces. Informatiebeveiliging is geïmplementeerd in al onze werkzaamheden.
- *Security by Design*
  Integrale aanpak informatiebeveiliging. Informatiebeveiliging is vanaf de start van ...? Een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.
- *Security by Default*
  Standaard beperkte toegang en veilige instellingen. Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.

Doelgroep

Het Informatiebeveiligingsbeleid is bestemd voor iedereen die – intern of extern – te maken heeft met de bedrijfsprocessen van Avans Hogeschool. Onderhavig beleid richt zich in eerste instantie op het College van Bestuur, de directies en leidinggevende alsmede het team Privacy en Security. Zij zijn verantwoordelijk voor de implementatie van het beleid, waardoor het beleid van toepassing wordt alle medewerkers, docenten, studenten, bestuurders, gasten, bezoekers en externe relaties.

Reikwijdte van het beleid

Bij Avans Hogeschool wordt informatiebeveiliging breed geïnterpreteerd. Het gaat over alle vormen van (formeel) vastgelegde informatie (dus niet alleen digitale informatie), die Avans Hogeschool genereert en beheert. Informatiebeveiliging strekt zich ook uit tot een groot deel van de toeleveranciers van Avans Hogeschool, aangezien zij in voorkomende gevallen een integraal onderdeel vormen van de bedrijfsprocessen en informatiestromen. De ketenverantwoordelijkheid impliceert dat Avans Hogeschool actief moet zorgen voor adequate beveiligingsmaatregelen bij haar toeleveranciers, om zo de integriteit, beschikbaarheid en vertrouwelijkheid van de door hen ten behoeve van Avans Hogeschool verwerkte informatie te waarborgen.

Het Informatiebeveiligingsbeleid heeft betrekking op alle academies, diensten en Centers of Expertises van Avans Hogeschool met onderliggende processen en systemen en de daarin of daarmee verwerkte data. Het beleid is van toepassing op alle door Avans Hogeschool beheerde apparaten en applicaties waarmee geautoriseerde toegang tot (diensten van) het Avans Hogeschool-netwerk kan worden verkregen en/of waarmee data van Avans Hogeschool wordt verwerkt.

Onder systemen (waaronder applicaties) vallen (deze lijst is niet uitputtend):

- Alle (fysiek) op het netwerk aangesloten apparaten zoals servers, werkstations, laptops, multi-functionals, laboratoriumapparatuur en gebouwbeheerssystemen.
- Alle draadloos op het netwerk aangesloten mobiele apparaten, zoals laptops, notebooks, tablets, en smartphones.
- IoT[7]-devices, zoals bewakingscamera's en sensoren.
- Alle op deze apparaten beschikbare (web/cloud)services en applicaties ('apps') die door Avans Hogeschool zijn ontwikkeld, aangeschaft en/of in licentie in gebruik zijn binnen de processen.

Avans Hogeschool faciliteert het gebruik van privéapparaten (BYOD[8]) voor zowel medewerkers, externen als

[7] Internet of Things
[8] Bring Your Own Device

studenten. Het gebruik van BYOD op het Avans Hogeschool-netwerk voor toegang tot applicaties of informatie van Avans Hogeschool valt onder dit Informatiebeveiligingsbeleid.

Het beleid is locatie-onafhankelijk: het geldt ook als men op een andere locatie dan op het terrein van Avans Hogeschool met informatie of informatievoorzieningen van Avans Hogeschool werkt (zoals thuis, in de trein of op hybride externe leeromgeving).

De impact van beide beleidskeuzes op de IT-dienstverlening door Avans is dat vanuit een informatiebeveiligingsperspectief hier moet worden gewerkt aan een zogenoemde 'Zero Trust' omgeving. Dit heeft vergaande impact op identiteiten(beheer) en (wederzijdse) authenticatie en autorisatie (per-sessie basis), beveiliging van de datacommunicatie alsmede logging en monitoring om goed zicht te hebben en houden op de kwaliteit van de informatiebeveiligingsstatus van de gehele omgeving.

Governance

Rollen en verantwoordelijkheden

Voor de governance van informatiebeveiliging in algemene zin naast de privacy-compliance verwerking van persoonsgegevens is een gelijkluidend model gekozen. De governance die is vastgelegd in het privacybeleid is ook van toepassing op het informatiebeveiligingsbeleid en daarom hier herhaald.

Om de informatiebeveiliging en verwerkingen van persoonsgegevens gestructureerd en gecoördineerd op te pakken, wordt bij Avans Hogeschool een aantal rollen onderkend die aan functionarissen in de bestaande organisatie zijn toegewezen.

College van Bestuur

Het College van Bestuur is eindverantwoordelijk voor informatiebeveiliging en de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen Avans Hogeschool en stelt dit beleid vast.

Portefeuillehouder privacy

De portefeuillehouder privacy is het lid van het College van Bestuur, dat bescherming van persoonsgegevens in zijn portefeuille heeft. De portefeuillehouder privacy is het eerste aanspreekpunt op bestuurlijk niveau voor privacyzaken en betrekt de Functionaris Gegevensbescherming tijdig bij aangelegenheden die verband houden met de bescherming van persoonsgegevens. Tevens is de portefeuillehouder privacy verantwoordelijk voor de regie op beleidsimplementatie. De portefeuillehouder privacy mandateert taken en bevoegdheden naar de beleidsverantwoordelijke eenheid.

Directeuren

Het bestuurs- en beheersreglement van Avans Hogeschool is leidend. Hierin staan de bevoegdheden en verantwoordelijkheden van een directeur beschreven. Een directeur is daardoor integraal verantwoordelijk voor compliance in zijn bedrijfsonderdeel, vanuit dit beleidsdocument op het gebied van informatiebeveiliging. Dit betekent dat hij proceseigenaar en verantwoordelijke is voor de aan hem gestelde mandaten en/of volmachten. Een directeur is verantwoordelijk voor de uitvoering en de implementatie van het beleid voor zijn bedrijfsonderdeel.

In relatie tot het informatiebeveiligingsbeleid is een directeur verantwoordelijk voor:

- het treffen van beveiligingsmaatregelen in lijn met het informatiebeveiligingsbeleid en de daaraan verbonden beleidsdocumenten, standaarden en procedures. Dit onder andere door ervoor te zorgen dat de ondersteunende applicatie(s) en bijbehorende ICT-faciliteiten een goede en veilige ondersteuning bieden aan het proces waar deze verantwoordelijk voor is;
- bewustwording van de medewerkers inzake informatiebeveiliging;
- het naar behoren en tijdig betrekken van de CISO bij aangelegenheden die verband houden met de bescherming van informatie die binnen de scope van dit informatiebeveiligingsbeleid valt waarvoor nog geen duidelijke beleidsrichtlijnen, standaarden of procedures beschikbaar zijn.

Beleidsverantwoordelijke eenheid

De Diensteenheid ICT en Facilitaire Dienst (DIF) is de beleidsverantwoordelijke eenheid voor dit beleid en is daarmee verantwoordelijk voor:

- de doorlopende ontwikkeling en actualisatie van het beleid;
- het monitoren van de implementatie en uitvoering van het beleid;
- het faciliteren van de organisatie door het beschikbaar stellen van standaarden en handreikingen waarin praktische vertaalslagen van dit beleid zijn opgenomen;

Functionaris Gegevensbescherming

Het College van Bestuur benoemt een Functionaris Gegevensbescherming en draagt zorg voor registratie van deze functionaris bij de Autoriteit persoonsgegevens. De Functionaris Gegevensbescherming is de interne toezichthouder op toepassing en naleving van de privacywetgeving én dit beleid, en adviseert de Verwerkingsverantwoordelijke. De Functionaris Gegevensbescherming rapporteert rechtstreeks aan de portefeuillehouder privacy van het College van Bestuur.

De Functionaris Gegevensbescherming heeft de volgende taken:

- de Functionaris Gegevensbescherming informeert en adviseert alle betrokken partijen over hun verplichtingen onder de privacywetgeving;
- de Functionaris Gegevensbescherming ziet toe op de naleving van de privacywetgeving en dit beleid;
- de Functionaris Gegevensbescherming adviseert over de manier waarop Verwerkingen rechtmatig, behoorlijk en transparant kunnen plaatsvinden, bijvoorbeeld op basis van het verwerkingsregister en aan de hand van Data Protection Impact Assessments;
- de Functionaris Gegevensbescherming is verplicht samen te werken met en op te treden als eerste aanspreekpunt van de Autoriteit persoonsgegevens;
- de Functionaris Gegevensbescherming neemt de ruimte om het College van Bestuur te informeren over zijn bevindingen inzake de naleving van de privacywet- en regelgeving.

Het College van Bestuur kent daarvoor de volgende bevoegdheden toe aan de Functionaris Gegevensbescherming:

- de Functionaris Gegevensbescherming heeft toegang tot alle informatie die nodig is om bovengenoemde activiteiten te kunnen vervullen;
- de Functionaris Gegevensbescherming krijgt de benodigde middelen om zijn deskundigheid in stand te houden;
- de Functionaris Gegevensbescherming mag andere taken en functies vervullen, mits die niet tot een belangenconflict kunnen leiden.

- De Functionaris Gegevensbescherming is werkzaam binnen de stafafdeling beleidsevaluatie en Control (BE&C).

CISO

De CISO (Chief Information Security Officer) is verantwoordelijk voor de professionalisering en borging van de informatiebeveiliging van Avans. Hieronder wordt verstaan de beveiliging van de informatievoorziening (waaronder IT-infrastructuur), het inzichtelijk maken van risico's Avans-breed, het opstellen van kaders, het monitoren van de naleving daarvan en het doen van verbetervoorstellen om het beveiligingsniveau continu te verbeteren. De CISO rapporteert integraal over informatiebeveiliging bij Avans aan het College van Bestuur. De CISO kan zowel gevraagd als ongevraagd advies geven. De directeur DIF (portefeuille ICT) is de hiërarchisch leidinggevende van de CISO.

Product Owner Privacy & Security (PO P&S)

De PO P&S vervult een rol bij de vertaling van de strategie naar tactische (operationele) en technische plannen en maatregelen. Dit doet hij samen met de CISO en met de systeem- en proceseigenaren. Tevens adviseert de PO P&S over specifieke informatiebeveiligingsmaatregelen, bijvoorbeeld in projecten, bij acquisities van software of hardware, etc. De PO P&S heeft directeur DIF (portefeuille ICT) als hiërarchisch leidinggevende en geeft op dagelijkse basis functioneel leiding aan het team van Security Officers en Privacy Officers. Naast de PO P&S zijn er decentraal meer functionarissen met de rol ICTO-Coaches. Deze functionarissen vertalen de centraal vastgestelde maatregelen en operationele plannen door naar de decentrale organisatie

Security Officer

De security officer maakt deel uit van het team Privacy & Security en helpt securityrisico's naar een acceptabel niveau te reduceren en heeft de volgende taken:

- de security officer informeert en adviseert over security aangelegenheden;
- de security officer monitort en bewaakt de opvolging van security incidenten;
- de security officer monitort de uitvoering door product teams van security policies;
- de security officer fungeert als vraagbaak voor andere (centrale) teams bij inrichtingsvraagstukken en daarmee samenhangende informatiebeveiligingseisen

Privacy Officer

De privacy officer maakt deel uit van het team Privacy & Security en helpt privacy risico's naar een acceptabel niveau te reduceren en heeft de volgende taken:

- de privacy officer informeert en adviseert over privacy aangelegenheden;
- de privacy officer bewaakt de kwaliteit van het verwerkingsregister;
- de privacy officer signaleert privacy risico's;
- de privacy officer adviseert bij het opstellen van Data Protection Impact Assessments en Privacy Risk Assessments;
- de privacy officer coördineert de afhandeling van verzoeken met betrekking tot rechten van Betrokkenen.

Privacy & Security (P&S) Contactpersoon

Alle academies en onderzoekscentra van Avans benoemen een Privacy & Security (P&S) contactpersoon. De rol is gekoppeld aan de rol van ICT-contactpersoon, tenzij de directeur van een bedrijfsonderdeel hier iemand anders (of anderen) voor aanwijst. De P&S contactpersoon is kennishouder van dit beleid en van interne informatiebeveiliging gerelateerde regelgeving. Hij weet wat zich in de haarvaten van de academie afspeelt en is eerste aanspreekpunt voor de academie op het gebied van informatiebeveiliging. De P&S contactpersoon heeft korte lijnen met collega's zodat risico's tijdig gesignaleerd kunnen worden. In voorkomende gevallen kan de P&S contactpersoon de security officer of de CISO raadplegen. Tevens zijn de P&S contactpersonen aanspreekpunten voor de Security Officers en de CISO.

De taken van de P&S contactpersoon zijn (in het kader van dit beleid):

- Het signaleren van vraagstukken op het gebied van informatiebeveiliging in de academie;
- Aanspreekpunt voor informatiebeveiligingsvragen binnen de academie/ het onderzoekscentrum;

- Het leveren van een bijdrage aan het bewustwordingsproces rondom informatiebeveiliging binnen de academie/ het onderzoekscentrum.

Juridische Zaken

Juridische Zaken verleent tweedelijns ondersteuning aan team Privacy (zoals is beschreven in het Protocol Juridische Advisering van Avans Hogeschool). Dat betekent dat privacy-gerelateerde vragen enkel bij Juridische Zaken terecht komen via team Privacy.

Three Lines of Defence

De Governance bij Avans Hogeschool is ingericht volgens het zogenaamde Three Lines of Defence model[9] (ook wel '3LoD'). Dit model wordt algemeen toegepast als model om Governance, Risk en Compliance (GRC) te borgen in een operationele organisatie. Het beschrijft niet alleen de rollen binnen de organisatiestructuur, maar ook hun onderlinge samenwerking.

Eerste lijn

Het 3LoD-model heeft als uitgangspunt dat het lijnmanagement (de business) verantwoordelijk is voor haar eigen processen. De directeuren zorgen ervoor dat privacy afspraken ook werkelijk worden geïmplementeerd, dat awareness programma's worden uitgevoerd, dat personeel wordt opgeleid, etc. Dit is de eerste lijn.

Tweede lijn

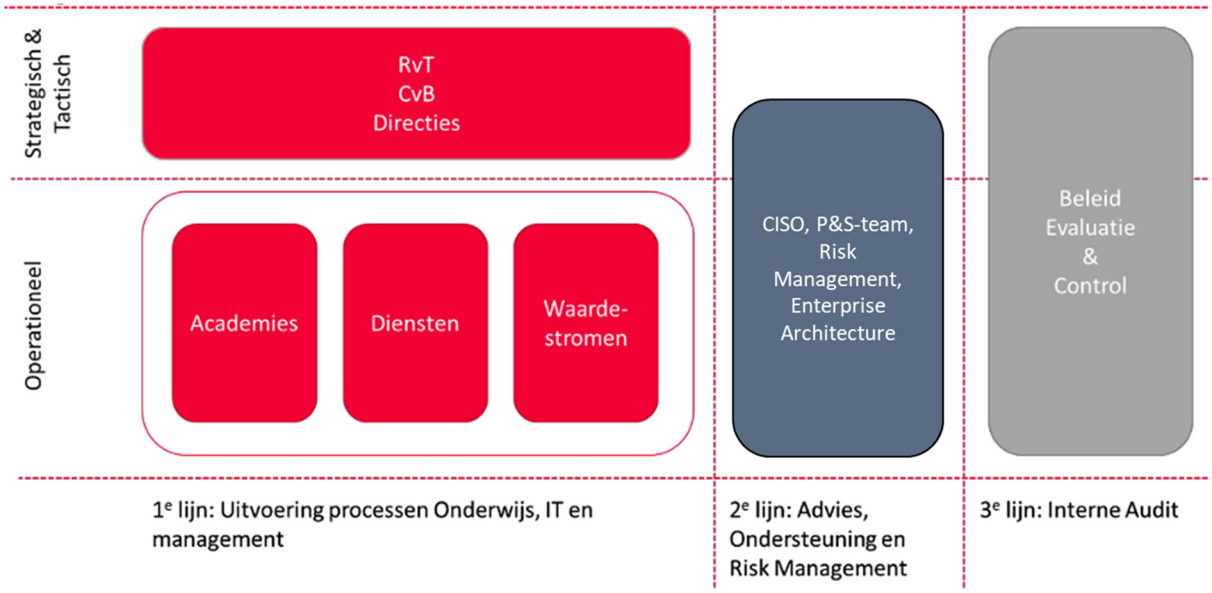
Daarnaast moet er een functie zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. Ook bepaalde beleidsvoorbereidende taken, het organiseren van de PDCA-cyclus, van integrale risicoanalyses en self-assessments en het opstellen van jaarplannen en rapportages zijn taken van de tweede lijn. De CISO, PO P&S, security officers en privacy officers bevinden zich in de tweede lijn.

De derde lijn

Het is wenselijk dat er binnen de organisatie een functie bestaat die controleert of het samenspel tussen de eerste en tweede lijn soepel functioneert en daarover een objectief, onafhankelijk oordeel velt met mogelijkheden tot verbetering. Daarbij kijkt de derde lijn ook of er geen overlapping is en of er blinde vlekken bestaan. Deze functie is de derde lijn.

De Functionaris Gegevensbescherming en de afdeling BE&C behoren tot de derde lijn. Beiden opereren volledig los van alle andere organisatieonderdelen en rapporteren niet alleen aan College van Bestuur, maar ook aan de Raad van Toezicht.

[9] https://www.icas.com/ca-today-news/internal-audit-three-lines-of-defence-model-explained



Verdeling van verantwoordelijkheden

Avans Hogeschool (Stichting Avans) wordt aangemerkt als Verwerkingsverantwoordelijke in de zin van de AVG. De feitelijke Verwerking van persoonsgegevens vindt echter op allerlei lagen van Avans plaats. Avans Hogeschool, vertegenwoordigd door het College van Bestuur, is eindverantwoordelijk voor de Verwerkingen van persoonsgegevens, waarvoor zij het doel en de middelen vaststelt.

Het zorgvuldig verwerken van persoonsgegevens dient gezien te worden als een lijnverantwoordelijkheid. Dat betekent dat de directeuren de primaire verantwoordelijkheid dragen voor een zorgvuldige Verwerking van persoonsgegevens op hun eenheid. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan. Onder de lijnverantwoordelijkheid valt ook de taak om het beleid te communiceren de medewerkers van de eenheid.

Het zorgvuldig omgaan met persoonsgegevens is ieders verantwoordelijkheid. In dit verband wordt van medewerkers en studenten verwacht dat zij zich integer gedragen. Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies van Avans Hogeschool of van individuen.

Bewustwording en kennis

beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om bij zowel medewerkers als studenten van Avans Hogeschool het privacy-bewustzijn en de kennis over zorgvuldige omgang met persoonsgegevens voortdurend aan te scherpen, zodat het bewustzijn van de risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

Bewustwording

Avans Hogeschool zet zich in om het privacy-bewustzijn te verhogen en daarna periodiek op te frissen en aan te scherpen, zodat (externe) medewerkers:

- de noodzaak inzien van privacyregels en -beleid;
- proactief en conform beleid en instructies handelen;
- elkaar aanspreken op mogelijke risico's en gedrag;
- weten hoe (beveiligings)incidenten moeten worden gemeld;
- bereid zijn om de dialoog aan te gaan met betrokkenen van Avans Hogeschool;
- voorbeeldgedrag tonen en zich bewust zijn van hun eigen gedrag;

- weten hoe en waar de informatie is te vinden om te kunnen werken conform dit beleid.

Avans Hogeschool onderneemt geregeld activiteiten om het privacy-bewustzijn bij (externe) medewerkers te verhogen en hoog te houden. Daarvoor worden bewustwordingscampagnes georganiseerd, zo mogelijk in combinatie met interne campagnes (bijvoorbeeld campagnes vanuit informatiebeveiliging). Voor de bewustwording van nieuwe medewerkers wordt zoveel mogelijk aangesloten bij reeds bestaande communicatiemomenten.

De beleidsverantwoordelijke eenheid (DIF) is eindverantwoordelijk voor het organiseren van Avans-brede bewustwordingscampagnes.

Kennis

Behalve bewustzijn op het gebied van informatiebeveiliging en privacy is het van belang dat (externe) medewerkers en studenten kennis hebben over wat bij Avans Hogeschool veilig en verantwoord gedrag is en wat niet.

Daarvoor stelt Avans Hogeschool een privacy & security website beschikbaar voor iedereen die onder de verantwoordelijkheid van Avans Hogeschool persoonsgegevens verwerkt of zijn kennis over privacy wil aanscherpen. De beleidsverantwoordelijke eenheid (DIF) is eindverantwoordelijk voor de totstandkoming, de verdere ontwikkeling en het onderhoud van de privacy & security website.

Controle en naleving PDCA-cyclus

De ambitie van Avans is dat dit beleid in opzet en bestaan aantoonbaar geïntegreerd is binnen haar bedrijfsvoering. Om dat mogelijk te maken, is inbedding in de PDCA-cyclus van belang. Onderdeel van een volledige PDCA-cyclus is het meten van de kwaliteit en het opstarten van verbeteracties. Met een PDCA-cyclus wordt ook inzichtelijk waar de organisatie staat met het voldoen aan wet- en regelgeving. Daarvoor wordt gebruik gemaakt van het SURFaudit Toetsingskader Privacy, welke Avans – evenals de PDCA-cyclus – heeft opgenomen in haar GRC-tool Trustbound.

Privacy management is opgenomen binnen de planning en control-cyclus van Avans. De Functionaris Gegevensbescherming doet jaarlijks verslag aan het College van Bestuur en geeft aanbevelingen voor een verdere optimalisering van de privacy beleidsvoering. Het College van Bestuur besluit over bijsturing van dit beleid in overeenstemming met de aanbevelingen van de Functionaris Gegevensbescherming.

Naleving

Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. Team beleidsevaluatie & Control (BE&C) initieert de interne controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens.

Controle, oefenen, naleving en sancties

Bij Avans Hogeschool is de afdeling beleidsevaluatie & Controle (BE&C) verantwoordelijk voor de (planning van) interne IT-audits en de CISO voor de controle op de uitvoering van de informatiebeveiligingsjaarplannen (samen met de PO P&S en zijn team van Security Officers alsmede de ICTO-Coaches).

De interne controles vinden jaarlijks plaats en worden naast de reguliere formele audits aangevuld met diverse incidentele activiteiten, zoals het nemen van steekproeven, het uitvoeren van penetratietesten en het controleren van de feitelijke werking van de vastgestelde beveiligingsmaatregelen.

De informatiesystemen (of -processen) van Avans Hogeschool worden intern geaudit. De audit richt zich op (1) de classificatie van de in het informatiesysteem vastgelegde gegevens (2), de inventarisatie van de risico's (3), de genomen beveiligingsmaatregelen en (4) de samenhang tussen 1, 2 en 3. Voor elk informatiesysteem wordt een audit frequentie vastgesteld aan de hand van de risicoclassificatie. Als een informatiesysteem wordt vervangen of als er belangrijke wijzingen plaatsvinden in de beveiliging, wordt er een audit uitgevoerd

op basis van een nieuwe business impact analyse en risicoanalyse. De externe controle wordt in een cyclus van twee jaar uitgevoerd door een onafhankelijke partij. Dit is qua planning gekoppeld met het accountantsonderzoek en dit wordt zoveel mogelijk gecombineerd met de normale planning & control-cyclus.

Het SURF IBHO Toetsingskader (zie hoofdstuk 3) wordt gebruikt als uitgangspunt voor interne en externe controles. Voor de audits van specifieke onderdelen of van informatiesystemen kunnen aanvullende, meer gedetailleerde, normen worden vastgesteld. Denk hierbij aan een kader voor ontwikkeling van veilige software.

Avans Hogeschool neemt deel aan de SURFaudit self-assessment cyclus en de bijbehorende jaarlijkse benchmark. Minimaal eens per 2/4 jaar wordt een Peerreview aangevraagd.

De bevindingen van de interne en externe controles en mogelijke externe eisen met betrekking tot beveiliging, zijn input voor de nieuwe jaarplannen van Avans Hogeschool. Deze kunnen ook tot wijziging van het Informatiebeveiligingsbeleid leiden (als onderdeel van de Act van de PDCA-cyclus).

Controle op de naleving door leidinggevenden vindt plaats door toezicht te houden op hoe in de dagelijkse praktijk met informatiebeveiliging wordt omgegaan. Hierbij is het van belang dat leidinggevenden (inclusief onderwijsverantwoordelijken) de medewerkers en studenten aanspreken op tekortkomingen. Voor het toezicht op de naleving van de AVG is de ‘Functionaris Gegevensbescherming’ (FG) verantwoordelijk. Dit wordt beschreven in het Avans Hogeschool Privacy beleid[10].

Als uit de controles blijkt dat de naleving ernstig tekortschiet, dan kan Avans Hogeschool de betrokken verantwoordelijke medewerkers of studenten een sanctie opleggen. De sanctie wordt opgelegd binnen de kaders van de cao, arbeidsovereenkomsten, integriteitscode en de wettelijke mogelijkheden in bijvoorbeeld de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW).

Financiering

Financiële middelen voor informatiebeveiliging worden structureel opgenomen in de diverse (project)begrotingen. De financiering van informatiebeveiliging wordt bij Avans Hogeschool centraal en decentraal geregeld.

Centraal

Algemene zaken, zoals het opstellen van een informatiebeveiligingsplan voor Avans Hogeschool of een externe audit, worden uit de algemene middelen betaald. Instelling brede bewustwordingscampagnes en trainingen worden ook uit deze middelen betaald.

Decentraal

De beveiliging van informatiesystemen en processen, inclusief de kosten daarvan, zijn integraal onderdeel van verantwoord beheer van het betreffende informatiesysteem of proces. Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten. Voorlichting en training voor specifieke toepassingen of doelgroepen worden uit decentrale middelen betaald.

[10] URL Avans Hogeschool Privacy beleid

Informatiebeveiligingsbeleidsstukken

Dit informatiebeveiligingsbeleid wordt nader ingevuld met een reeks van verdiepende policies en standaarden. Hierbij wordt, zoals vanuit de SURF / ISO27001 benadering verwacht, in ieder geval gewerkt met de volgende policies:

- Informatiebeveiligingsbeleid (dit beleid)
- beleid voor toegangscontrole
- beleid inzake beheer van informatie-assets
- beleid inzake risicobeheer
- beleid inzake classificatie en verwerking van informatie
- Bewustmakings- en opleidingsbeleid op het gebied van informatiebeveiliging
- beleid inzake aanvaardbaar gebruik
- beleid voor opgeruimde werkplek (screen en desk)
- beleid inzake mobiel en telewerk
- Bedrijfscontinuïteitsbeleid
- Back-up beleid
- Malware- en antivirusbeleid
- beleid voor wijzigingsbeheer
- Beveiligingsbeleid van externe leveranciers (derde partijen)
- beleid voor continue verbetering
- beleid inzake logging en monitoring
- beleid voor het beheer van netwerkbeveiliging
- beleid inzake informatieoverdracht
- Veilig ontwikkelingsbeleid
- Fysieke beveiligingsbeleid
- beleid voor cryptografisch sleutelbeheer
- Cryptografisch controle- en versleutelingsbeleid
- beleid inzake incidentmanagement
- beleid voor patchbeheer
- beleid voor cloudservices

Naleving van het beleid

Meting van naleving

Het team Privacy & Security zal de naleving van dit beleid verifiëren door middel van verschillende methoden, inclusief maar niet beperkt tot rapporten over bedrijfstools, interne en externe audits en feedback aan de beleidseigenaar.

Uitzonderingen

Elke uitzondering op het beleid moet vooraf worden goedgekeurd en vastgelegd door de CISO en worden gerapporteerd aan het Risicoteam-overleg.

Niet-naleving

Een persoon die dit beleid heeft overtreden, kan worden onderworpen aan disciplinaire maatregelen.

Vaststelling & wijziging

Het College van Bestuur stelt, met instemming van de medezeggenschapsraad, het Informatiebeveiligingsbeleid vast dat de Chief Information Security Officer (CISO) voorstelt. Het Informatiebeveiligingsbeleid volgt de kaders van het instellingsbeleid. Minimaal 1 keer per 4 jaar, of na een substantiële verandering van het instellingsbeleid of belangrijke ontwikkelingen op cyberveiligheidsgebied, wordt het beleid herzien en opnieuw vastgesteld.

Dit beleid, versie 1.03, is vastgesteld door het College van Bestuur van Avans Hogeschool op 9 april 2024 en kan worden aangehaald als “Informatiebeveiligingsbeleid van Avans Hogeschool”.

Bijlage A – Relatie informatiebeveiliging en privacy

Naast dit informatiebeveiligingsbeleid is ook een privacy beleid beschreven binnen Avans. Informatiebeveiliging en privacy zijn onderling verbonden, maar verschillen onderling ook. De onderstaande tabel geeft een beknopt overzicht van die verbondenheid en de verschillen.

Binnen Avans gelden de termen privacy en informatiebeveiliging als synergetische, overlappende onderwerpen. Heb je het over privacy, dan bedoel je vaak informatiebeveiliging, en visa versa. Privacy gaat echter over het correct, voor een bepaald doel, gebruiken van verzamelde persoonsgegevens. Informatiebeveiliging daarentegen draait om de inspanningen die we verrichten om te zorgen dat deze gegevens vertrouwelijk, integer en beschikbaar blijven.	
Informatiebeveiliging	**Privacy**
Informatiebeveiliging omvat alle gegevens van een organisatie.	Privacy gaat alleen over persoonsgegevens.
Informatiebeveiliging beschermt de organisatie	Privacy beschermt de mensen
Informatiebeveiliging is gericht op de belangen van de organisatie zelf. Het doel van het informatiebeveiligingsbeleid is om de continuïteit van de organisatie te waarborgen, en te voorkomen dat gevoelige informatie op straat komt te liggen.	Privacy is erop gericht de rechten en vrijheden van natuurlijke personen te beschermen en beschermt mensen binnen en buiten de organisatie tegen misbruik van hun gegevens. Ook tegen overmatig gebruik van de gegevens door de organisatie zelf.
Informatiebeveiliging zorgt ervoor dat beveiligingsincidenten, zoals datalekken, adequaat worden opgelost.	Vanuit privacy is het belangrijk om datalekken op te lossen. Hiervoor bestaat de afhankelijkheid van informatiebeveiliging waar beveiligingsincidenten (inclusief datalekken) worden opgelost.
Informatiebeveiliging leunt op drie kernbegrippen: vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Samen bepalen zij de betrouwbaarheid van informatie- systemen binnen de organisatie.	Privacy is erop gericht dat iedere verwerking van persoonsgegevens binnen de organisatie rechtmatig plaatsvindt. De kernbegrippen vertrouwelijkheid, integriteit en beschikbaarheid spelen wel een rol binnen privacy, maar vormen niet de kern.
De organisatie van informatiebeveiliging is een cyclisch proces op basis van de Plan-Do-Check Act-cyclus. De organisatie krijgt hierdoor steeds beter grip op informatiebeveiliging en verbetert continu. Hiervoor bestaat een internationale richtlijn ISO 27001 voor een Information Security Management System (ISMS). Binnen Avans wordt momenteel gewerkt in de geest van ISO 27001.	Waar voor informatiebeveiliging de PDCA-aanpak al geruime tijd gemeengoed is ontbreekt dit voor privacy. Sinds enkele jaren bestaat internationaal de ISO 27701 als privacy-uitbreiding van de ISO 27001.De ISO 27701 beschrijft een Privacy Information Management System (PIMS). Binnen Avans vindt integratie van privacy management plaats in het ISMS. Avans beraadt zich momenteel nog of zij zich op termijn ook voor ISO 27701 wil certificeren.
Informatiebeveiliging is binnen Avans strategisch georganiseerd op basis van het Three Lines of Defense principe. Meer uitleg hierover is beschreven in hoofdstuk 4. De CISO heeft hierbinnen een centrale rol vanuit de tweede lijn voor advies, ondersteuning en controle. De CISO wordt ondersteund door een team van Security Officers in de IT-operatie. De uitvoerende verantwoordelijkheid ligt bij de Diensten en Academies. De eindverantwoordelijkheid ligt bij het CvB.	Privacy is eveneens georganiseerd op basis van het Three Lines of Defense principe. De Privacy Officer heeft een vergelijkbare rol als de CISO voor informatiebeveiliging. En die wordt ondersteund door een team van Privacy Officers. Een verschil met de organisatie voor informatiebeveiliging is de rol van de Functionaris Gegevensbescherming (FG). De FG heeft een onafhankelijke beschermde rol om Avans als organisatie als geheel te kunnen ondersteunen, adviseren en beoordelen op het vlak van privacy beleid en-beheer.

Bijlage B – Wet- en regelgeving

Avans Hogeschool zorgt ervoor te allen tijde in haar processen procedures te voldoen aan onderstaande relevante wet- en regelgeving, voor zover dit relatie heeft tot (het) informatiebeveiliging(sbeleid).

Wetgeving

Naam	Bron / vindplaats
Aanbestedingswet 2012	https://wetten.overheid.nl/BWBR0032203/2019-01-01
Archiefwet	https://wetten.overheid.nl/BWBR0007376/2022-05-01/0
Auteurswet	https://wetten.overheid.nl/BWBR0001886/2018-10-11
AVG / GDPR	https://wetten.overheid.nl/BWBR0040940/2019-02-19
Cookieswet (=wijziging Telecommunicatiewet)	https://www.eerstekamer.nl/behandeling/20141007/gewijzigd_voorstel_van_wet
eIDAS verordening	https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32014R0910&from=EN
Uitvoeringswet AVG	https://wetten.overheid.nl/BWBR0040940/2020-01-01
Wetboek van strafrecht (n.a.v. de Wet Computercriminaliteit	http://wetten.overheid.nl/BWBR0019934/2007-09-01 https://wetten.overheid.nl/BWBR0041368/2019-03-01/0
Wet op de identificatieplicht	https://wetten.overheid.nl/BWBR0006297/2017-03-01
Wet op de inlichtingen- en veiligheidsdiensten 2017	https://wetten.overheid.nl/BWBR0039896/2018-05-01

Regelgeving

Naam	Bron / vindplaats
Basisselectie document WO	
EU-richtlijn Netwerk en informatiebeveiliging (NIB)	https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016L1148&from=NL
Handreiking betrouwbaarheidsniveaus	https://www.forumstandaardisatie.nl/sites/default/files/BFS/4-basisinformatie/publicaties/fs-handreiking-betrouwbaarheidsniveus-v4_0.pdf
Richtsnoer beveiliging persoonsgegevens	https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_beveiliging_van_persoonsgegevens.pdf

Normen en aanwijzingen

Naam	Bron / vindplaats
Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek	https://www.vsnu.nl/code-pers-gegevens.html
ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection	https://www.iso.org/standard/54534.html
Nederlandse gedragscode wetenschappelijke integriteit	https://www.vsnu.nl/files/documenten/Nederlandse gedragscode wetenschappelijke integriteit 2018.pdf
SURF Toetsingskader informatiebeveiliging	https://www.surf.nl/diensten/surfaudit