Beleidsnotitie Informatiebeveiliging en Privacy

Helicon Opleidingen

Vastgesteld door CvB op 6 november 2017

Verantwoording

Bron:
Starterkit Informatiebeveiliging
Stichting SURF
Februari 2015
Herkomst Kennisnet

Bewerkt door:
Kennisnet / saMBO-ICT (IBPDOC6, versie 2.0 juli 2016)

Bewerkt voor Helicon Opleidingen door:
drs. P.G.M. Kremers, concerncontroller
17 maart 2017

Voorzien van een positief advies van:
Adviescommissie Informatisering
22 maart 2016 (eerdere versie)

Vastgesteld door:
College van Bestuur
Voorlopig besluit 27 maart 2017
Definitief besluit 6 november 2017

Inhoudsopgave

Inleiding

1.1 Informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van de informatievoorziening te garanderen. Deze kwaliteitsaspecten zijn niet vrij te interpreteren maar zijn strikt gedefinieerd en dus niet op verschillende manieren uit te leggen. (zie bijlage 1)

Informatiebeveiliging is een beleidsverantwoordelijkheid van het bestuur van Helicon Opleidingen. Ook in het onderwijsveld is sprake van toenemende afhankelijkheid van informatie en computersystemen, waardoor nieuwe kwetsbaarheden en risico's kunnen optreden. Het is daarom van belang hiertegen adequate maatregelen te treffen. Immers, onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van het onderwijs en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagoverlies.

Helicon Opleidingen heeft de ambitie om informatiebeveiliging structureel naar een hoger niveau te brengen en daar op te houden door de aspecten governance, wet- en regelgeving, de organisatie van de beveiligingsfunctie en het informatiebeveiligingsbeleid – ook in hun onderlinge relatie – duidelijk in dit document te beschrijven en vast te stellen.

1.2 Privacy

Het privacy beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Helicon Opleidingen, waaronder in ieder geval alle medewerkers, leerlingen, stagiairs, gasten, bezoekers en externe relaties (o.a. inleen), evenals op andere betrokkenen waarvan Helicon Opleidingen persoonsgegevens verwerkt.

In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van Helicon Opleidingen, alsmede op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Eveneens is het beleid van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens, die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Bij Helicon Opleidingen wordt het beschermen van persoonsgegevens breed geïnterpreteerd. Er is een belangrijke relatie en forse overlap met het aanpalende beleidsterrein informatiebeveiliging, waarbij het gaat om de beschikbaarheid, integriteit en de vertrouwelijkheid van data, waaronder persoonsgegevens. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht.
Het beleid bij Helicon Opleidingen heeft als doel om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene wordt gerespecteerd. De gegevens, die betrekking hebben op een betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik dan wel misbruik op basis van het fundamenteel recht op bescherming van zijn/haar persoonsgegevens. Dit brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens veilig zijn bij Helicon Opleidingen.

1.3 Vervlechting informatiebeveiliging en privacy

In de reikwijdte van het beleid wordt beschreven wat de afbakening is van het toepassingsgebied. Bij Helicon Opleidingen wordt informatiebeveiliging (processen) gekoppeld aan privacy (mensen). Het IBP-beleid binnen Helicon Opleidingen heeft betrekking op alle medewerkers, leerlingen, gasten, geregistreerde bezoekers en externe relaties en op alle organisatieonderdelen. Tevens vallen onder het IBP-beleid alle devices van waaraf geautoriseerde toegang tot het instellingsnetwerk verkregen kan worden.
Bij het IBP-beleid ligt de nadruk op die toepassingen die vallen onder de verantwoordelijkheid van Helicon Opleidingen. Dit heeft zowel betrekking op *gecontroleerde informatie*, die door de instelling zelf is gegenereerd en wordt beheerd, als ook op *niet-gecontroleerde informatie*, (bijv. informatie in een personal workspace op Vibe, uitspraken van leerlingen of personeel in discussies), waarop de instelling kan worden aangesproken.

1.4 Doelstelling informatiebeveiligings- en privacy-beleid

Het IBP-beleid bij Helicon Opleidingen heeft als doel het waarborgen van de continuïteit van de bedrijfsvoering en het minimaliseren van de schade door het voorkomen van beveiligings- en privacy-incidenten (preventie) en het minimaliseren van eventuele gevolgen (schadebeperking).

Het doel van het IBP-beleid voor Helicon Opleidingen is concreet het volgende:

Kader: het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan een vastgestelde best practice of norm en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen.

Normen: de basis voor de inrichting van het informatiebeveiligingsbeleid is ISO 27001 (Eisen aan Managementsystemen voor Informatiebeveiliging).

Maatregelen worden op basis van best practices in het mbo en hoger onderwijs en o.b.v. ISO 27002 genomen (Code voor Informatiebeveiliging)

Expliciet: uitgangspunten en organisatie van informatiebeveiligings- en privacy- (verwerken persoonsgegevens) functies zijn vastgelegd en worden gedragen door het College van Bestuur, en afgeleid daarvan, door de hele organisatie.

Daadkrachtig: daadkrachtige implementatie van het beleid door duidelijke keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering van beleidsmaatregelen.

Compliance: het informatiebeveiligingsbeleid biedt de basis om te voldoen aan wettelijke voorschriften. Het privacybeleid is compliant met de Nederlandse en Europese wetgeving.

Door het concretiseren van IBP-beleid op het procesniveau van Helicon Opleidingen wordt aantoonbaar dat dit beleid bijdraagt aan de realisering van de overall doelstellingen die Helicon Opleidingen voor zichzelf heeft geformuleerd *('alignment').* Die doelstellingen zijn het bieden van een kwalitatief hoogwaardige onderwijsomgeving, die bijdraagt aan de verbetering van de kwaliteit van de samenleving als geheel. Deze omgeving behoort veilig te zijn en te voldoen aan relevante wet- en regelgeving.

1.5 Beschermen van persoonsgegevens

Naast bovenstaande concrete doelstellingen is een meer algemeen doel het instelling breed creëren van bewustwording van het belang en de noodzaak van het beschermen van persoonsgegevens, mede ter vermijding van risico's als gevolg van het niet compliant zijn met de relevante wet- en regelgeving.

Opslag en verwerking van persoonsgegevens is noodzakelijk om te voldoen aan wettelijk voorgeschreven uitwisselingen van gegevens en voor de bedrijfsprocessen van Helicon Opleidingen. Dit dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van persoonsgegevens grote schade kan berokkenen aan leerlingen, medewerkers en andere betrokkenen bij Helicon Opleidingen, maar ook bij Helicon Opleidingen zelf. Helicon Opleidingen hecht dan ook veel waarde aan het beschermen van de persoonsgegevens die aan haar worden verstrekt en aan de wijze waarop persoonsgegevens worden verwerkt. Het op een juiste manier verwerken van persoonsgegevens is de verantwoordelijkheid van het bestuur van Helicon Opleidingen.

Met het beschrijven van de maatregelen in dit beleidsdocument beoogt en neemt Helicon Opleidingen haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacywet- en regelgeving.

Het is van belang om het door Helicon Opleidingen gevoerde IBP-beleid ook bekend te maken aan leerlingen en medewerkers, alsmede om de visie daarover breed uit te dragen. Hiervoor is het gebruik van een privacyreglement (soms ook wel privacy-statement genoemd) een goed middel. Dit document beschrijft op welke wijze Helicon Opleidingen omgaat met persoonsgegevens van leerlingen en medewerkers, en wat ieders rechten en verplichtingen zijn. Alhoewel het gebruik van een privacyreglement niet wettelijk is voorgeschreven, is dit toch als bijlage toegevoegd. Dit reglement is evenals het beleidsplan vastgesteld door het CvB en heeft de instemming van de Ondernemingsraad gekregen.

2. Beleidsuitgangspunten en principes

2.1 Beleidsuitgangspunten informatiebeveiliging en privacy

IBP-beleid wordt op procesniveau geïmplementeerd en uitgevoerd. Dat houdt in dat de jaarlijkse planning en control cyclus gebaseerd is op ISO 27001 (Plan, Do, Check, Act of Analyse, Ambitie, Activiteitenplan). Hierin worden jaarplannen opgesteld en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen.

Het belangrijkste beleidsuitgangspunt bij Helicon Opleidingen is dat we een open, transparante en toegankelijke instelling zijn.

Dit open en toegankelijk karakter heeft betrekking op gasten, maar ook op leerlingen en medewerkers. Deze open benadering van informatievoorziening en -gebruik, ICT en beveiliging heeft echter met name voor interne gebruikers ook consequenties. Er wordt van medewerkers en leerlingen verwacht dat ze zich qua techniek en ook qua houding ‘fatsoenlijk’ gedragen (eigen verantwoordelijkheid). Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Het is om deze reden dat er gedragscodes zijn geformuleerd, vastgesteld en geïmplementeerd.
De informatiebeveiliging en het privacy beleid dienen te voldoen aan de relevante wet- en regelgeving, in het bijzonder aan de Algemene Verordening Gegevensbescherming (AVG 2016).
Hierbij dient een goede balans te worden aangebracht tussen het belang van Helicon Opleidingen om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens.

2.2 Aanvullende uitgangspunten

Naast het bovenstaande beleidsuitgangspunt hanteert Helicon Opleidingen de volgende aanvullende uitgangspunten:

- Informatiebeveiliging en privacy is een lijnverantwoordelijkheid: dat betekent dat de proceseigenaren de primaire verantwoordelijk dragen voor een goede informatiebeveiliging en privacy ten aanzien van (proces gebonden) informatie die op hun afdeling / eenheid wordt gebruikt dan wel gegenereerd. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan.
- Veilig en betrouwbaar omgaan met informatie in het dagelijkse werk is ieders professionele verantwoordelijkheid. Verwachtingen t.a.v. individuen: communiceer met medewerkers, leerlingen, docenten en derden dat er van hen verwacht wordt dat ze actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie. Dat gebeurt in de aanstellingsbrief, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera. Het opleggen van sancties na ernstige overtredingen maakt het geheel geloofwaardig.
- Informatiebeveiliging en privacy zijn een continu proces. Regelmatige herijking van beleid en audits: technologische en organisatorische ontwikkelingen binnen en buiten de instelling maken het noodzakelijk om periodiek te bezien of men nog wel op de juiste wijze bezig is de beveiliging te waarborgen. De audits maken het mogelijk het beleid en de genomen maatregelen te controleren.
- Eigendom van informatie: de onderwijsinstelling is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de instelling informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen dienen goed geïnformeerd te zijn over de regelgeving voor het (her)gebruik van deze informatie.

- Houderschap van informatie: in opdracht van eigenaar, houdt en beheert de houder de informatie middels een informatiesysteem (applicatie) en ziet toe op juiste classificatie, middels risico analyse, van het informatiesysteem op gebieden van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). De houder wordt in de gelegenheid gesteld (middelen) om de uit classificatie voortvloeiende maatregelen, te (laten) implementeren.
- Bij projecten, zoals infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met informatiebeveiliging en privacy ("privacy by design").

2.3 Privacy principes

Om aan bovenstaande beleidsuitgangspunten te voldoen gelden de volgende privacy principes:

Grondslag
- Verwerking van persoonsgegevens is gebaseerd op een van de **wettelijke grondslagen**, zoals genoemd in artikel 8 van de Wet bescherming persoonsgegevens (Wbp).

Doel
- Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en **gerechtvaardigde doeleinden**. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd.

Doelbinding
- Persoonsgegevens worden **niet *verder* verwerkt** op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
- Verwerking van persoonsgegevens gebeurt op **de minst ingrijpende wijze** en dient in redelijke verhouding te staan tot het beoogde doeleinde.

Data-minimalisatie
- Bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de persoonsgegevens die **strikt noodzakelijk** zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn.
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens **juist en actueel** zijn.
- Persoonsgegevens worden **niet *langer* verwerkt** dan noodzakelijk is voor de doeleinden van de verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen.

Transparantie
- Iedere betrokkene heeft **recht op inzage** respectievelijk verbetering, aanvulling, verwijdering of afscherming van de in de afzonderlijke verwerkingen hem betreffende persoonsgegevens, en heeft het recht van verzet.
- De instelling kan aan betrokkenen op transparante wijze **verantwoording** afleggen over welke gegevens er allemaal verzameld worden en over de verwerkingen daarvan en de daarbij gehanteerde principes.
- Bij alle registraties op vrijwillige basis zal aan de betrokkene na toestemming een eenduidige zogenaamde **Opt-out[1] procedure** worden aangeboden

Overig:
Persoonsgegevens worden **adequaat beveiligd** volgens de geldende beveiligingsnormen

[1] Zie Algemene Verordening Gegevensbescherming

3. Classificatie

Belangrijk aspect bij informatiebeveiliging en privacy is de classificatie van gegevens. Hierbij wordt in beeld gebracht wat het belang van diverse (sets van) gegevens is opdat er een adequate beveiliging aan gegeven kan worden. Hierbij is het doel om de risico's die de instelling loopt bij de verwerking van deze gegevens zo klein mogelijk te maken.

3.1 Risico's

De proceseigenaren van Helicon Opleidingen zijn de aangewezen verantwoordelijken om besluiten te nemen rond classificatie van de gegevens die in hun proces een rol spelen. En daarmee geven ze aan welke risico's aanvaardbaar zijn en welke moeten worden verkleind. De proceseigenaren zien de grootste risico's op de volgende gebieden en hebben aangegeven deze met prioriteit te willen aanpakken:

- Ongewenste verspreiding van zorgdossiers van leerlingen.
- Ongewenste verspreiding van verslagen voortvloeiend uit de gesprekscyclus (functioneren, beoordelen, etc.).
- Ongecontroleerde toegang tot het netwerk en applicaties.
- Verlies van privacy gevoelige data (datalekken).

Deze risico's worden gemitigeerd door beleid, training en classificatie.

3.2 Gehanteerde classificatie standaard

Helicon Opleidingen hanteert de classificatie standaarden zoals die verwoord zijn in het Certificeringsschema Informatiebeveiliging en Privacy, dat wordt beheerd binnen Edustandaard. Deze standaard is onderdeel van de Referentie Onderwijs Sector Architectuur (ROSA).[2]

Bij Helicon Opleidingen zijn of worden alle gegevens waarop dit informatiebeveiligingsbeleid van toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse.
De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses.
Daarbij zijn de volgende kwaliteitsaspecten van informatievoorziening van belang:

Beschikbaarheid: De mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ICT-dienstverlening waarborgen.

Integriteit: De mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.

Vertrouwelijkheid: De mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.

A. Beschikbaarheid
Ten aanzien van de beschikbaarheidseisen is voor de volgende classificatie indeling gekozen:

Classificatie	Gevolg
Laag	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **1 week** brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, medewerkers, leerlingen, ouders of klanten.
Midden	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **48 uur** brengt merkbare schade toe aan de belangen van de instelling, medewerkers, leerlingen, ouders of klanten.
Hoog	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **4 uur** brengt merkbare schade toe aan de belangen van de instelling, medewerkers, leerlingen, ouders of klanten.

[2] Een initiatief van Kennisnet.

B. Integriteit
Voor integriteit wordt de volgende indeling gevolgd:

Classificatie	Gevolg
Laag	Het bedrijfsproces staat **enkele** integriteitsfouten toe
Midden	Het bedrijfsproces staat **zeer weinig** integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk
Hoog	Het bedrijfsproces staat **geen** integriteitsfouten toe.

C. **Vertrouwelijkheid**
Vertrouwelijkheid is ingedeeld in de volgende klassen:

Classificatie	Gevolg
Laag	Informatie mag of moet toegankelijk zijn voor **alle of grote groepen** medewerkers, leerlingen, ouders of klanten. Vertrouwelijkheid is gering. Voorbeeld is de website van Helicon Opleidingen.
Midden	Informatie mag alleen toegankelijk zijn voor een **beperkte groep** gebruikers. De informatie is vertrouwelijk.
Hoog	Informatie is zeer vertrouwelijk, alleen bedoeld voor **specifiek benoemde personen**, waarbij onbedoeld bekend worden buiten deze groep grote schade kan toe brengen.

Welk beveiligingsniveau geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt. De classificatie dient door de proceseigenaar te worden bepaald.
Deze classificatie wordt samengevat tot BIV (Beschikbaarheid-Integriteit-Vertrouwelijkheid), waar vervolgens door de proceseigenaren scores aan worden toegevoegd.

Binnen onderwijsinstellingen krijgt beschikbaarheid over het algemeen de classificatie “Midden”, maar kunnen integriteit en vertrouwelijkheid sterk verschillen per proces.

Voorbeeld: Zo zou de proceseigenaar onderwijs het zorgdossier kunnen classificeren met Integriteit en Vertrouwelijkheid Hoog. Kort weergegeven als BIV-MHH. Het gelabelde proces zorgdossier wordt geclassificeerd MHH.

4. Wet- en regelgeving

4.1 Wettelijke voorschriften

Bij Helicon Opleidingen wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

4.1.1 Wet Educatie en Beroepsonderwijs (WEB)

Helicon Opleidingen heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de leerlingen administratie en met de studieresultaten is gewaarborgd.

4.1.2 Algemene Verordening Gegevensbescherming (AVG)

Helicon Opleidingen heeft de wettelijke vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) geïmplementeerd via het IBP-beleid. Vanaf 1 januari 2016 geldt dit ook voor de Meldplicht Datalekken. De ingangsdatum van de AVG is 25 mei 2016 en de inwerkingtreding is 25 mei 2018. De AVG komt in plaats van de Wbp (Wet bescherming persoonsgegevens).

4.1.3 Archiefwet

Helicon Opleidingen houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d. Dit is onderdeel van de jaarlijkse externe accountantsrapportages. (zie ook het basis selectiedocument voor de MBO sector.)

4.1.4 Auteurswet

Helicon Opleidingen verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat Helicon Opleidingen het gebruik van software zonder het bezitten van de juiste licenties tegen gaat.

4.1.5 Wetboek van Strafrecht

In het Wetboek van Strafrecht zijn de laatste decennia een aantal specifieke bepalingen opgenomen over de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet schrijft voor dat “enige beveiliging” vereist is alvorens er sprake *kan zijn* van het eventueel strafrechtelijk vervolgen van delicten jegens de onderwijsinstelling en het eventueel vrijwaren van bestuurders van de instelling. Naleving van dit informatiebeveiligingsbeleid en implementatie van de basis maatregelen bij Helicon Opleidingen moet leiden tot een niveau van beveiliging dat als voldoende mag worden gezien in het kader van het Wetboek van Strafrecht.

4.2 Overige richtlijnen en landelijke afspraken

Zoals eerder gesteld is het informatiebeveiligingsbeleid bij Helicon Opleidingen gebaseerd op ISO 27001. Helicon Opleidingen voldoet aan de volgende richtlijnen en landelijke afspraken:

- DUO afspraken Bron e.d.;
- Aansluitvoorwaarden SURFnet;
- Bepalingen uit de CAO;
- Verantwoord Gebruik van het Netwerk (VGN, ook wel AUP, acceptable use policy genoemd). Dit is een formele aanvulling op de arbeidsovereenkomst.

5. Governance IB-beleid

Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term governance. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de instelling, zoals de eigenaren, werknemers, leerlingen, andere afnemers en de samenleving als geheel. Een goed corporate governance-beleid draagt zorg voor de rechten van alle belanghebbenden.

5.1 Afstemming met aanpalende beleidsterreinen

Onderdeel van governance is dat aan alle soorten risico's en hun onderlinge verwevenheid passende aandacht geschonken wordt. Het is om die reden dat bij Helicon Opleidingen op strategisch niveau zowel aandacht geschonken wordt aan informatiebeveiliging, als aan privacy beleid, fysieke beveiliging, ARBO-veiligheid en bedrijfscontinuïteit. Immers, samenwerking tussen deze disciplines is een noodzakelijke voorwaarde voor governance.
Dit is vormgegeven door de (budgettaire) planningscyclus voor deze aspecten parallel te laten verlopen. Dat biedt handvatten om onderlinge interferentie op te merken en te behandelen. Waar wenselijk en mogelijk wordt deze afstemming ook vertaald naar het tactische en operationele niveau, maar alleen daar waar het toegevoegde waarde biedt. In dit hoofdstuk wordt verder uitsluitend ingegaan op IT-governance en de positionering van informatiebeveiliging daarin.

5.2 Inpassing IB governance

In deze paragraaf wordt beschreven hoe IB-governance binnen Helicon Opleidingen is georganiseerd en wie waarvoor verantwoordelijk is. Van belang daarbij is om onderscheid te maken naar richtinggevend of strategisch, sturend of tactisch en uitvoerend niveau.
De Manager **I**nformatie**B**eveiliging en **P**rivacy (afgekort als manager IBP) is een rol op strategisch, tactisch en uitvoerend niveau. Hij adviseert, samen met de Informatiemanager, aan het College van Bestuur. De manager IBP bewaakt de uniformiteit binnen de instelling.
Op de vestigingen zijn de taken van de manager IBP op het ondersteunend niveau belegd bij daartoe aangewezen functionarissen. Deze vervullen een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit doen ze samen met de eigenaren van de technische platforms.
Op operationeel niveau wordt overlegd met de functionele (functioneel beheer financiën en functionele beheerders van administratieve en educatieve applicaties) en technische beheerders. Er wordt aandacht geschonken aan de implementatie van de maatregelen in het kader van de informatiebeveiliging en privacy.

Schematisch weergegeven:

Niveau	*Wat?*	*Wie?*	*Overleg*	*Documenten*
Richting-gevend	• *Bepalen IBP strategie* • *Organisatie t.b.v. IBP inrichten* • *IB-planning en control vaststellen* • *Business continuity management*	• *CvB, i.c Portefeuillehouder IBP, o.b.v. advies Manager IBP*	*CvB stelt vast Directeurenberaad en Medezeggenschap adviseren*	• *IBP beleidsplan* • *IBP baseline (basis maatregelen)* • *Business continuity plan*
Sturend	• *Planning & Control IBP:* · *voorbereiden* · *normen en wijze van toetsen* · *evalueren beleid en maatregelen* · *begeleiding externe audits*	• *Proces eigenaar* • *Manager IBP* • *Functioneel beheerders* • *Functionaris Gegevens-bescherming*	*Tactisch IBP in de Adviescommissie Informatisering*	• *Risicoanalyses en audits* • *Jaarplan en verslag*
Uitvoerend	• *Implementeren IBP-maatregelen* • *registreren en evalueren incidenten* • *communicatie eindgebruikers*	• *Functioneel Beheerder* • *Automatisering* • *Communicatie*	*Operationeel IBP-overleg in Centraal Functioneel Beheer Overleg en Platform Systeembeheer*	• *SLA's (security paragraaf)* • *Incident-registratie, incl. evaluatie*

De financiering van informatiebeveiliging en privacy wordt bij Helicon Opleidingen als volgt geregeld. Algemene zaken, zoals het opstellen van een IBP-plan voor de gehele instelling of een externe audit, worden uit het centrale IBP-budget betaald. De beveiliging van informatiesystemen komt ten laste van het informatiesysteem zelf.
Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten. Het zelfde geldt voor awareness en training: er kunnen instelling brede bewustwordingscampagnes zijn (centraal gefinancierd) en lokale voorlichting en training voor specifieke toepassingen of doelgroepen (decentraal gefinancierd).

5.3 Documenten informatiebeveiliging

Voor informatiebeveiliging wordt bij Helicon Opleidingen dezelfde management-cyclus gevolgd, die ook voor andere onderwerpen geldt: beleid, analyse, plan implementatie, uitvoering, controles en evaluatie.

5.3.1 Het informatiebeveiligings- en privacy-beleid

Het IBP-beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen de instelling. In het IBP-beleid worden de randvoorwaarden en uitgangspunten vastgelegd en de wijze waarop het beleid wordt vertaald in concrete maatregelen. Om er voor te zorgen dat het beleid gedragen wordt binnen de organisatie en de organisatie er naar handelt wordt het uitgedragen door (of namens) het College van Bestuur. Het informatiebeveiliging en privacy beleid wordt opgesteld door de manager IBP en vastgesteld door het College van Bestuur.

5.3.2 Baseline van maatregelen (basisniveau maatregelen)

Deze baseline beschrijft de maatregelen die minimaal nodig zijn om instelling breed een minimaal niveau van informatiebeveiliging en privacy te kunnen waarborgen. Dit vloeit voort uit het beleid of uit besluiten die door het tactisch overleg genomen zijn. Deze basis maatregelen dienen dus overal in de instelling genomen te worden. De baseline wordt gemaakt door de manager IBP en goedgekeurd door het College van Bestuur. Wanneer er systemen zijn die na een risicoanalyse hogere beveiligingseisen nodig hebben, dan worden deze bovenop de minimale maatregelen genomen.

5.3.3 Jaarplan/verslag

Elk jaar levert de manager IBP een jaarverslag en een jaarplan voor het volgende jaar. Het jaarplan is mede gebaseerd op de resultaten van de periodieke controles / audits. Er wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (incl. genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Dergelijke verslagen kunnen geconsolideerd worden in de bestuurlijke Planning & Control-cyclus.

5.3.4 Business Continuity Plan

Business Continuity Management (BCM) is de benaming van het proces dat potentiële bedreigingen voor een organisatie identificeert en bepaalt wat de impact op de “operatie” van de organisatie is, als deze bedreigingen daadwerkelijk manifest worden. Het product van BCM bestaat uit een samenhangend stelsel van maatregelen, die zowel preventief, detectief, repressief als correctief werkzaam zijn. Het Business Continuity Plan wordt opgesteld door de manager IBP, in samenwerking met de proceseigenaren en de informatiemanager.

5.3.5 Diensten niveau overeenkomsten (SLA’s)

Een service level agreement is een overeenkomst tussen een leverancier en een afnemer. Bijvoorbeeld de ICT-afdeling sluit met externe leveranciers een SLA af t.b.v. de ondersteuning van concernsystemen. Dat zijn contracten met afspraken en randvoorwaarden over geleverde diensten. In deze contracten zit standaard een IBP-paragraaf, waarin de verantwoordelijkheden van de leverancier zijn opgenomen.

5.3.6 Contracten applicaties en educatieve software

Met alle leveranciers van onderwijs- en bedrijfsapplicaties en educatieve software worden bewerkersovereenkomsten afgesloten. Dit geldt ook voor overheids- en ander instellingen indien er data van studenten of medewerkers wordt verstrekt, al dan niet op wettelijke basis.

5.3.7 Inhuur- en uitbestedingscontracten

Bij de inhuur van diensten en personeel van derde partijen zal ook aandacht aan informatiebeveiliging en privacy besteed moeten worden, bijvoorbeeld door te stellen dat het instellingsbeleid ook van toepassing is voor hen en door het sluiten van bewerkersovereenkomsten of het overeenkomen van geheimhoudingsbedingen. Hetzelfde is van belang bij uitbestedingen.

5.3.8 Policies[3]

Gedragscodes en richtlijnen voor medewerkers, leerlingen en derden, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging.
Zoals:

- Acceptable use policy, voor het veilig gebruik van ICT-voorzieningen;
- Wachtwoordpolicy;
- Toepassing van crypto grafische hulpmiddelen;
- Classificatierichtlijnen;
- Policy voor het afsluiten van servers en werkstations;
- Integriteit- en gedragscode voor ICT-functionarissen;
- Gedragscode voor veilig e-mail en internetgebruik;
- Protocol social media.

5.4 Controle, naleving en sancties

Bij Helicon Opleidingen initieert de manager IBP de controle op de uitvoering van de IBP-jaarplannen. De externe controle wordt (in de toekomst) uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning & Control cyclus.
Steeds vaker is er ook sprake van branche audits, zoals de MBO-audit (afgeleid van de HO-Audit en bewerkt door Kennisnet en saMBO-ICT). De bevindingen van de interne en externe audits zijn input voor de nieuwe jaarplannen van Helicon Opleidingen.
De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP-proces. Van belang hierbij is dat lijnmanagers hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Voor de bevordering van de naleving van wettelijke bepalingen (WBP/AVG) vervult de Functionaris Gegevensbescherming (FG; binnen Helicon Opleidingen de manager IBP in een dubbel rol) een belangrijke rol. Deze wordt ingesteld door het College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het CvB vast te stellen reglement. Mocht de naleving ernstig tekort schieten, dan kan Helicon Opleidingen de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.5 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij Helicon Opleidingen het bewustzijn (Awareness) voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Zulke campagnes kunnen aansluiten bij landelijke campagnes in het mbo en hoger onderwijs, zo mogelijk in afstemming met beveiligingscampagnes voor ARBO, milieu en fysiek. Verhoging van het beveiligings-bewustzijn is een verantwoordelijkheid van de manager IBP, maar uiteindelijk is ook hiervoor het College van Bestuur eindverantwoordelijk.

[3] Voor een aantal van deze policies is gebruik gemaakt van documenten uit mbo framework IBP.

5.6 Organisatie van de informatiebeveiliging en privacy

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Helicon Opleidingen een aantal rollen onderkend die aan functionarissen in de bestaande organisatie zijn toegewezen.

College van Bestuur
Het College van Bestuur stelt het beleid en de basis maatregelen op het gebied van informatie-beveiliging en privacy vast. Het collegelid dat informatiebeveiliging en privacy in zijn portefeuille heeft is eindverantwoordelijk voor informatiebeveiliging en privacy binnen Helicon Opleidingen.
De inhoudelijke verantwoordelijkheid voor informatiebeveiliging en privacy is gemandateerd aan de manager IBP. Deze heeft de opdracht om voor de informatiebeveiliging en privacy voor de gehele instelling zorg te dragen.

Manager IBP
De manager IBP is een rol op strategisch (en tactisch) niveau. Hij adviseert, samen met de Informatiemanager, aan het College van Bestuur. De manager IBP bewaakt de uniformiteit binnen de instelling.

Information Security Officer
De information security officer (ISO) is verantwoordelijk voor de fysieke beveiliging van de informatie binnen de instelling en het treffen van beheersmaatregelen, met als doel de continuïteit van de instelling te waarborgen en gevolgen van eventuele beveiligingsincidenten te beperken.

Informatiemanager
De informatiemanager adviseert over specifieke informatiebeveiligingsmaatregelen in projecten (hogere systemen) en bewaakt de consistentie van de maatregelen.

Functioneel beheerder
De rol van functioneel beheerder onderwijs- of bedrijfsapplicatie is bij Helicon Opleidingen centraal belegd. De functioneel beheerders (diverse personen) vervullen een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit doen zij samen met de Manager IBP, met de Information Security Officer (vanwege de uniformiteit) en met de systeem-eigenaren.

Proces-eigenaar
Een proces eigenaar is iemand die verantwoordelijk is voor een van de primaire of ondersteunende processen, zoals inkoop, HRM en onderwijs. (diverse personen)

Systeem-eigenaar
De systeemeigenaar is er verantwoordelijk voor dat een applicatie een goede ondersteuning biedt aan het proces waarvoor deze verantwoordelijk is. Dit betekent dat de systeemeigenaar er voor zorgt dat zowel nu als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving. Uiteraard moet de applicatie voldoen aan het informatie-beveiligingsbeleid en tenminste aan de basismaatregelen. (diverse personen)

Leidinggevende
Naleving van het IBP-beleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het IBP-beleid;
- toe te zien op de naleving van het IBP- beleid door zijn medewerkers;
- periodiek het onderwerp informatiebeveiliging en privacy onder de aandacht te brengen in werkoverleggen;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligings-en privacy-zaken.

De leidinggevende kan hierin ondersteund worden door de manager IBP.

Functionaris gegevensbescherming
De functionaris voor de gegevensbescherming (FG) houdt binnen Helicon Opleidingen toezicht op de toepassing en naleving van de Wet Bescherming Persoonsgegevens. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie (dubbelrol voor manager IBP; ondersteund door juridisch medewerker).

CERT-coördinator
Het hoofd Automatisering vervult de rol van CERT-coördinator bij Helicon Opleidingen. Hij is bevoegd het isoleren van computersystemen of netwerksegmenten te gelasten.

5.7 Overleg

Om de samenhang in de organisatie van de IBP-functie goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van informatiebeveiliging binnen de verschillende onderdelen op elkaar af te stemmen wordt bij Helicon Opleidingen gestructureerd overleg gevoerd over het onderwerp informatiebeveiliging op meerdere niveaus.

Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging en privacy. Dit gebeurt in het strategisch ICT-overleg. (CvB en directeuren)

Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. (Adviescommissie Informatisering)

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm is deels decentraal georganiseerd op het niveau van de vestiging, maar ook op instellingsniveau. (Centraal Functioneel Beheer Overleg / Platform Systeembeheer)

Voor alle drie de typen overleg geldt dat het zoveel mogelijk ingepast moet worden in bestaande overlegvormen met hetzelfde karakter. Zo zal op strategisch niveau niet alleen over informatiebeveiliging gesproken worden, maar ook over andere risico's waarmee de instelling te maken kan krijgen, zoals bijvoorbeeld financieel, personeel en continuïteit.

5.8 Uitwerking van het IBP-beleid

Op basis van het vastgestelde IBP-beleid is een projectgroep IBP belast met de verdere uitwerking. Belangrijke elementen die hierbij worden meegenomen zijn:

1. Een beoordeling van de startpositie voor Helicon Opleidingen. Wat is er al geregeld, wat moet er worden opgepakt, in welke volgorde en met welke prioriteit?
2. Baseline/basisniveau van maatregelen (zie paragraaf 5.3.2). Beschrijving van de maatregelen die minimaal getroffen dienen te worden om instelling breed een minimaal niveau van informatiebeveiliging en privacy te kunnen waarborgen.
3. Communicatieplan. Het opzetten van een plan om de bewustwording bij medewerkers, leerlingen en gasten te verhogen en vervolgens op niveau te houden.

De projectgroep bestaat uit:
Manager IBP (voorzitter)
Informatiemanager
Information Security Officer
Juridisch medewerker
Beleidsmedewerker Communicatie

6. Melding en afhandeling van incidenten

6.1 Registratie incidenten informatiebeveiliging en privacy

Incidentbeheer en -registratie hebben betrekking op de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging en privacy door de medewerkers en leerlingen gemeld worden en de wijze waarop deze worden afgehandeld.
Het is van belang om te leren van incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een volwassen informatiebeveiligingsomgeving. Bij Helicon Opleidingen is er daarom een meldpunt[4] ingericht en is bekend gemaakt hoe dat is te benaderen.
De lijnmanager dient de incidenten en inbreuken direct te melden aan het IBP Meldpunt Datalekken datalek@helicon.nl.
De meldplicht datalekken is per 1 januari 2016 opgenomen in de WBP. In het Protocol Datalekken heeft Helicon Opleidingen beschreven op welke wijze datalekken bij de toezichthouder (de Autoriteit Persoonsgegevens) moeten worden gemeld. Dit dient binnen 2 werkdagen te gebeuren. Op het niet (tijdig) melden van datalekken staat een boete. Als de privacy van betrokkenen is geschaad, moeten ook zij worden geïnformeerd over het datalek. De korte meldingstermijn is de reden dat in het protocol procesafspraken zijn vastgelegd en dat de Functionaris Gegevensbescherming is aangewezen om deze melding te doen.

6.2 Informatiebeveiligings- en Privacy-Crisis Team

Het doel van het Informatiebeveiligings- en Privacy-Crisis Team (IPCT) bij Helicon Opleidingen is instelling brede preventie en curatieve zorg voor informatiebeveiligings- en privacy-incidenten. Het IPCT houdt zich ook bezig met beveiligingsincidenten buiten Helicon Opleidingen als daar eigen medewerkers of leerlingen in enige rol bij betrokken zijn.
Een optie is om in zulke gevallen gebruik te maken van de diensten van SURFcert, die wereldwijd in verbinding staat met andere CERT's (Computer Emergency Response Team).

De leden van het IPCT zijn benoemd door het College van Bestuur en opereren in zijn opdracht. Het IPCT is gerechtigd het isoleren van computersystemen of netwerksegmenten te gelasten.

Het IPCT van Helicon Opleidingen heeft de volgende opdracht:

- Het signaleren en registreren van alle beveiligingsincidenten en datalekken, het coördineren van de bestrijding en het toezien op de oplossing van problemen die tot incidenten hebben geleid of door de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;
- Het leveren van managementrapportages over de beveiligings-incidenten en het doen van voorstellen tot betere preventie van of curatie op incidenten.

In geval van een incident levert het IPCT bij Helicon Opleidingen de volgende diensten:

- Afhandelen van binnenkomende e-mails
- Afhandelen van binnenkomende telefoons
- Inrichten en operationeel houden van een meldpunt voor alle beveiligingsincidenten en het coördineren en bewaken van een adequate afhandeling daarvan.
- Bekend maken van de bereikbaarheid van het IPCT (tijden/middelen) aan alle betrokkenen.
- Geven van voorlichting aan IT-gebruikers, -ontwikkelaars en -beheerders over preventie van incidenten en actuele bedreigingen
- Adviseren over instelling brede beveiligingsaspecten
- Periodiek opstellen van managementrapportages;
- Onderhouden van contacten met SURFcert.

[4] Incidenten worden bij Helicon Opleidingen geregistreerd in Topdesk

Het IPCT bij Helicon Opleidingen behandelt meldingen vertrouwelijk en verstrekt alleen informatie over informatiebeveiligings- en privacy-incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.
De dienstverlening van het IPCT bij Helicon Opleidingen is gedocumenteerd en door het College van Bestuur bekrachtigd. De rol van IPCT coördinator is belegd bij de manager IBP.

Het IPCT van Helicon Opleidingen kent de volgende samenstelling:

Manager IBP	coördinator
Juridisch medewerker	ondersteuning/secretariaat
Informatiemanager	
Information Security Officer	
CERT-coördinator	
Beleidsmedewerker communicatie	crisiscommunicatie

Bijlage 1: Kwaliteitsaspecten Informatiebeveiliging

Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid

Beschikbaarheid: de mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ICT-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is.
- Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is.
- Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

Integriteit: de mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd.
- Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is.
- Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Vertrouwelijkheid: de mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.
Deelaspecten hiervan zijn:

- Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is.
- Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is.
- Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn.
- Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

Controleerbaarheid: de mogelijkheid om kennis te verkrijgen over de structurering (documentatie) en werking van de IT-dienstverlening.
Deelaspecten hiervan zijn:

- Testbaarheid: De mate waarin de integere werking van de IT-dienstverlening te testen is.
- Meetbaarheid: Zijn er voldoende meet- en controlepunten aanwezig.
- Verifieerbaarheid: De mate waarin de integere werking van een IT-dienstverlening te verifiëren is.

Hierbij gaat het ook om de controleerbaarheid van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

Bijlage 2: Personele invulling IBP

Helicon Opleidingen heeft de verschillende functies/rollen binnen het IBP-beleid belegd bij eigen medewerkers. Hieronder is de situatie per 1 maart 2017 weergegeven:

Medewerker	**Functie binnen Helicon**	**Rol binnen het IBP-beleid**
dr.ir. A.F. Groen	voorzitter college van bestuur	portefeuillehouder informatiebeveiliging
drs. P.G.M. Kremers	concerncontroller	manager IBP functionaris gegevensbescherming coördinator IPCT
H.J. Burg MEd	informatiemanager	informatiemanager
A.L. Peeters	beleidsmedewerker ICT en beheer	information security officer
T. Backx	hoofd automatisering	CERT- coördinator
mr. F.J.G. Verhagen	juridisch medewerker	juridisch medewerker
S.A.J. Ragas	senior beleidsmedewerker communicatie	beleidsmedewerker communicatie