ONDERWIJSGROEP TILBURG

Informatiebeveiligings en Privacy beleid

Onderwijsgroep Tilburg

Documentsoort:	Beleid
Eigenaar:	Fred van der Westerlaken
Auteur:	J. Kolen, J. de Bruijn
Datum Vaststelling:	18 mei 2020
Document Id:	CvB/1920.023, BB 029

Inhoud

1 Inleiding

1.1 Informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een aantal samenhangende maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van de informatievoorziening te garanderen. Informatiebeveiliging richt zich op de volgende kwaliteitsaspecten:

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

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

Informatiebeveiliging is de (beleids-)verantwoordelijkheid van het College van Bestuur van Onderwijsgroep Tilburg. Het onderwijs is in toenemende afhankelijkheid van informatie- en computersystemen, waardoor kwetsbaarheden en risico's kunnen optreden. Het is daarom belangrijk hiertegen adequate technische en beveiligingsmaatregelen te nemen. Immers, onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van het onderwijs en de bedrijfsvoering.

1.2 Privacy

Het privacy beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Onderwijsgroep Tilburg. De betrokkenen zijn in ieder geval alle medewerkers, studenten, leerlingen en externe relaties, evenals anderen waarvan de persoonsgegevens worden verwerkt. Hierbij ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde en systematische verwerking van persoonsgegevens. De verwerking van persoonsgegevens vindt plaats onder de (eind-) verantwoordelijkheid van het College van Bestuur (als verwerkingsverantwoordelijke). De gegevensbescherming (privacy) geldt ook voor de niet-geautomatiseerde verwerking van persoonsgegevens, zoals papieren documenten.

Bij Onderwijsgroep Tilburg wordt de bescherming van persoonsgegevens breed geïnterpreteerd. Er is namelijk een belangrijke relatie en grote samenhang 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 vindt zowel planmatig, als inhoudelijk afstemming plaats. Het beleid is bedoeld 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.

1.3 Informatiebeveiligings- en privacy beleid (IBP-beleid)

Binnen Onderwijsgroep Tilburg worden informatiebeveiliging en privacy aan elkaar gekoppeld, omdat deze aanpalende beleidsterreinen onlosmakelijk met elkaar zijn verbonden. Het informatiebeveiligings- en privacy beleid (IBP-beleid) wordt breed geïnterpreteerd en heeft betrekking op alle medewerkers, studenten, leerlingen en externe relaties, maar ook op gasten en geregistreerde bezoekers. Tevens vallen onder het informatiebeveiligings- en privacy beleid alle devices van waaraf geautoriseerde toegang tot het instellingsnetwerk verkregen kan worden.

Bij het informatiebeveiligings- en privacy beleid ligt de nadruk op die toepassingen die vallen onder de verantwoordelijkheid van Onderwijsgroep Tilburg. Dit heeft zowel betrekking op gecontroleerde informatie, die door de instelling zelf is gegenereerd en wordt beheerd, als ook op niet-gecontroleerde informatie, zoals uitspraken van studenten in discussies, persoonlijke websites op externe social media waarin men zich profileert als werknemer, waarop de instelling kan worden aangesproken.

1.4 Doelen van IBP-beleid

Het informatiebeveiligings- en privacy beleid (IBP-beleid) heeft als doel:

- het waarborgen van de continuïteit van de onderwijsuitvoering en bedrijfsvoering;

- het minimaliseren van de schade door het voorkomen van beveiligings- en privacy-incidenten en het minimaliseren van eventuele gevolgen; en
- het garanderen van de privacy van alle betrokkenen van wie persoonsgegevens worden verwerkt, waaronder studenten en leerlingen, diens ouders/verzorgers en medewerkers.

Concreet biedt het informatiebeveiligings- en privacy beleid voor Onderwijsgroep Tilburg:

- het kader om (toekomstige) technische en organisatorische beheersmaatregelen in de informatiebeveiliging en privacy aan te toetsen en om de taken, bevoegdheden en verantwoordelijkheden rondom deze beleidsterreinen in de organisatie te beleggen (governance). De uitgangspunten en organisatie van informatiebeveiliging en privacy functies zijn vastgelegd en worden gedragen door het College van Bestuur, en afgeleid daarvan, door de hele organisatie.
- de basis voor de inrichting van het informatiebeveiligingsbeleid zijnde NEN-ISO/IEC-normen 27001 en 27002, en van het privacy beleid is dat de Algemene Verordening Gegevensbescherming (AVG). Het informatiebeveiligings- en privacy beleid biedt de basis om te voldoen aan de geldende wet- en regelgeving en normeringen (compliance).

Naast bovenstaande concrete doelstellingen is een meer algemeen doel het organisatie-breed creëren van bewustwording van het belang en de noodzaak van informatiebeveiliging en het beschermen van persoonsgegevens. De bewustwording is mede nodig ter voorkoming van privacy risico's voor medewerkers, studenten en leerlingen. Het is van belang om het door Onderwijsgroep Tilburg gevoerde informatiebeveiligings- en privacy beleid ook bekend te maken aan medewerkers, studenten en leerlingen, en uit te dragen. Hiervoor is het gebruik van een privacy reglement en een ICT gedragscode een goed middel. Het reglement beschrijft op welke wijze Onderwijsgroep Tilburg omgaat met persoonsgegevens van medewerkers, studenten en leerlingen en wat ieders rechten en verplichtingen zijn. In de ICT gedragscode staan de rechten en verplichtingen ten aanzien van informatiebeveiliging.

1.5 Uitgangspunten van IBP-beleid

Onderwijsgroep Tilburg hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het College van Bestuur neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het College van Bestuur is hierop aan te spreken en legt hier verantwoording over af als verwerkingsverantwoordelijke.
2. Informatiebeveiliging en privacy is een lijnverantwoordelijkheid. Dit betekent dat schooldirecteuren en hoofden de primaire verantwoordelijkheid dragen voor een goede informatiebeveiliging en gegevensbescherming ten aanzien van informatie en persoonsgegevens, die op hun school of afdeling worden gebruikt. Dit omvat de uitvoering en handhaving van beheers- en beveiligingsmaatregelen.
3. Onderwijsgroep Tilburg voldoet aan alle relevante wet- en regelgeving.
4. Bij Onderwijsgroep Tilburg is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van de organisatie om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming in- en herzien.
5. Onderwijsgroep Tilburg zal alle betrokkenen helder en actief informeren over de verwerkingen van hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, aanvullen, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit, afscherming en profilering van hun persoonsgegevens.
6. Onderwijsgroep Tilburg legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal dit register up-to-date houden, zoals benoemd in de AVG.
7. Binnen Onderwijsgroep Tilburg is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van een ieder. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.

8. Onderwijsgroep Tilbug neemt bij verwerkingen van persoonsgegevens geen volledig geautomatiseerde besluiten (waaronder profilering) die voor de betrokkene rechtsgevolgen heeft of betrokkene in aanmerkelijke mate treft. Bij geautomatiseerde besluitvorming wordt binnen Onderwijsgroep Tilburg altijd een menselijke toets uitgevoerd.
9. Onderwijsgroep Tilburg is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en studenten worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
10. Onderwijsgroep Tilburg classificeert informatiesystemen en gegevens. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.
11. Onderwijsgroep Tilburg sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als, in opdracht van de organisatie, persoonsgegevens worden verwerkt.
12. Onderwijsgroep Tilburg verwacht van alle medewerkers, studenten en leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Onderwijsgroep Tilburg heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
13. Informatiebeveiliging en privacy is bij Onderwijsgroep Tilburg een continu kwaliteitsproces, waarbij regelmatig (minimaal jaarlijks) wordt ge-audit of een self assessment (zoals Benchmark IBP) wordt uitgevoerd en wordt gekeken of een aanpassing gewenst dan wel noodzakelijk is.
14. Onderwijsgroep Tilburg kijkt bij wijzigingen (denk ook aan uitfasering) in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.
15. Onderwijsgroep Tilburg neemt passende technische en/of organisatorische (beveiligings-) maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de bedrijfsvoering en de privacy kunnen verstoren.
16. Onderwijsgroep Tilburg zal alle beveiligingsincidenten en datalekken vastleggen, volgens een vast protocol afhandelen en indien nodig melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.
17. Onderwijsgroep Tilburg kiest ten aanzien van informatiebeveiliging (autorisatie en authenticatie) voor de vooronderstelling "Alles is in principe verboden tenzij het uitdrukkelijk is toegelaten" in plaats van de zwakkere regel "Alles is in principe toegelaten tenzij het uitdrukkelijk is verboden". De uitgangspunten voor identificatie, authenticatie en autorisatie zijn te vinden in ons vastgestelde IAA-Beleid.

2 Compliance

Dit hoofdstuk geeft een invulling en uitwerking van bovenstaande uitgangspunten om te voldoen aan de geldende wet- en regelgeving en dus compliant te zijn.

2.1 Relevante wet- en regelgeving

De uitwerking van dit beleid voldoet aan alle geldende van toepassing zijnde wet- en regelgeving, waaronder (niet limitatief):

- Wet Educatie en Beroepsvorming (WEB) en Wet Voortgezet Onderwijs (WVO)
- Branche codes Goed Bestuur VO en MBO
- Wet Inspectietoezicht
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Auteurswet
- Wetboek van Strafrecht
- Koppelingswet

Het internationale normenkader voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beheers- en beveiligingsmaatregelen. Daarnaast wordt ook gebruik gemaakt van in het onderwijs toegepaste standaarden zoals het ROSA certificeringsschema.

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake de omgang met persoonsgegevens (artikel 5 van de AVG) leidend. Deze zijn samengevat in de vijf vuistregels van de AVG en worden door Onderwijsgroep Tilburg gevolgd.

Onderwijsgroep Tilburg hanteert het Toetsingskader en Framework Informatiebeveiliging en Privacy dat ontwikkeld is door saMBO-ICT, Kennisnet en SURF.

De bepalingen uit de meest recente versie van het convenant ‘Digitale onderwijsmiddelen en privacy’ zijn leidend bij het maken van afspraken met leveranciers van digitale leermiddelen en examens, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

2.2 Reglementen en procedures

Diverse aanvullende beleidsstukken, reglementen, gedragscodes en procedures geven invulling aan de uitwerking van het IBP-beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende documenten. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd in actuele dataregisters.

2.3 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico’s op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hierbij een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico’s wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en leerlingen en de presentaties voor (groepen van) medewerkers. Verhoging van het bewustzijn is de verantwoordelijkheid van elke leidinggevende en wordt gefaciliteerd door de IM, de FG en de CIB.

2.4 Classificatie en risicoanalyse

Alle gegevens en informatiesystemen waarop dit beleid van toepassing is worden geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid (BIV-classificatie) de kwaliteitscriteria die van belang zijn.

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Hiervoor worden DPIA’s uitgevoerd (Data Protection Impact Assessment).

Vanaf de start van nieuwe (ICT-) projecten of wijzigingen in applicaties, wordt rekening gehouden met informatiebeveiliging en privacy.

2.5 Incidenten en datalekken

Alle medewerkers die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht van datalekken. Alle (beveiligings-)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings-)incidenten kunnen worden gemeld bij de servicedesk.

Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

Ook aan studenten en externen is gecommuniceerd op welke manier zij kwetsbaarheden en incidenten dienen te melden.

2.6 Planning en controle

Dit IBP-beleid wordt tweejaarlijks getoetst, geëvalueerd en eventueel bijgesteld door het College van Bestuur. Hierbij wordt rekening gehouden met:

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

De tweejaarlijkse cyclus wordt ook gehanteerd bij de aanvullende documenten (in bijlage 1).

Daarnaast kent Onderwijsgroep Tilburg een jaarlijks actieplan voor informatiebeveiliging en privacy. Aan de hand van de resultaten uit het Toetsingskader en de Benchmark IBP en de actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving e.d. wordt het IBP-jaarplan gemaakt. Op basis van het Toetsingskader IBP vindt minimaal jaarlijks een interne beoordeling plaats door middel van self-assessment, peer-review en/of interne audit. Indien nodig, kunnen ook externe controles worden uitgevoerd door een onafhankelijke externe auditor.

2.7 Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Naleving van het IBP-beleid is een primaire verantwoordelijkheid van alle medewerkers, studenten en leerlingen binnen Onderwijsgroep Tilburg. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en medewerkers, studenten en leerlingen aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP-zaken door middel van periodieke bewustwordingscampagnes, gedragscodes e.d. Mocht de naleving van dit beleid ernstig tekortschieten, dan kan Onderwijsgroep Tilburg de betrokken verantwoordelijke medewerkers of studenten en leerlingen een sanctie op leggen binnen de kaders van de CAO of de reglementen.

Voor het toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt benoemd door het College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

2.8 Logging en monitoring

Door middel van logging en monitoring worden gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (pogingen tot) ongeautoriseerde toegang tot het netwerk. Onderwijsgroep Tilburg beoordeelt deze logbestanden met regelmaat.

2.9 Verwerkersovereenkomsten

De wetgeving verplicht Onderwijsgroep Tilburg om verwerkersovereenkomsten af te sluiten met 'verwerkers'. Verwerkers zijn externe leveranciers die op enige manier toegang of beschikking hebben tot persoonsgegevens van Onderwijsgroep Tilburg. Met verwerkers van onderwijs- en bedrijfsapplicaties en educatieve software worden daarom verwerkersovereenkomsten afgesloten. Dit geldt ook voor overheids- en andere instellingen indien er data van studenten of medewerkers wordt verstrekt, al dan niet op wettelijke basis.

2.10 Inhuur-, uitbestedings- en overige contracten

Bij de inhuur van diensten en personeel van derde partijen en bij uitbesteding wordt aandacht besteed aan informatiebeveiliging en privacy door de relevante instellingsbeleid- en regels, het inkoopbeleid en de algemene inkoopvoorwaarden van toepassing te laten zijn, en het sluiten van verwerkers-overeenkomsten en het overeenkomen van geheimhoudingsbedingen.

Onderwijsgroep Tilburg blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt. Aangezien leveranciers namens ons informatie verwerken is het logisch om hier eisen aan te stellen. De doelstelling daarvan is:

- De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.
- Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.

Eisen aan ICT leveranciers

Bij de selectie van ICT leveranciers of de voortzetting van ICT contracten, dienen de leveranciers zoveel mogelijk te voldoen aan de volgende eisen:

- De leverancier is in het bezit van een ISO 27001 certificaat, of laat jaarlijks de informatiebeveiliging testen in een assurance rapportage (bijvoorbeeld een SOC2 rapport, ISAE 3000 rapport of een ISAE 3402 rapport).
- De leverancier heeft een eigen informatiebeveiligingsbeleid en kan deze laten zien.
- De leverancier accepteert het ‘right to audit’ zodat Onderwijsgroep Tilburg kan (laten) controleren dat aan beveiligingseisen die van toepassing zijn, voldaan wordt. Een TPM kan als vervanging dienen van de gevraagde audit als de scope toereikend is.
- De leverancier werkt met capabele en integere medewerkers, welke tevens geheimhouding hebben ten aanzien van de informatie en data welke betrekking hebben op Onderwijsgroep Tilburg.

Eisen aan SaaS-applicaties

Bij de selectie van een SaaS- applicatie, dienen de leveranciers zoveel mogelijk te voldoen aan de volgende eisen:

- De leverancier is in het bezit van een ISO 27001 certificaat en/ of laat jaarlijks de informatiebeveiliging testen in een assurance rapportage (bijvoorbeeld een SOC2 rapport, ISAE 3000 rapport of een ISAE 3402 rapport).
- De leverancier heeft een eigen informatiebeveiligingsbeleid en kan deze laten zien.
- De leverancier heeft een eigen privacy beleid en kan deze laten zien.
- De leveranciers laat minimaal 1 x per jaar een penetratietest uitvoeren op de webfacing systemen van de SaaS-applicatie.
- De leverancier accepteert het ‘right to audit’ zodat Onderwijsgroep Tilburg kan (laten) controleren dat aan beveiligingseisen die van toepassing zijn, voldaan wordt. Een TPM kan als vervanging dienen van de gevraagde audit als de scope toereikend is.
- De leverancier werkt met capabele en integere medewerkers, welke tevens geheimhouding hebben ten aanzien van de informatie en data welke betrekking hebben op Onderwijsgroep tilburg.
- De leverancier draagt zorg voor een Escrow, zodat de mogelijkheid geborgd is dat de software onderhouden en gebruikt kan blijven worden in geval van bv. een faillissement.

3 Governance

In dit hoofdstuk wordt beschreven hoe IBP-governance in Onderwijsgroep Tilburg is georganiseerd en wie verantwoordelijk is waarvoor.

3.1 Rollen en verantwoordelijkheden

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden binnen Onderwijsgroep Tilburg een aantal rollen en verantwoordelijkheden onderscheiden.

College van Bestuur

Het College van Bestuur is eindverantwoordelijk voor de informatiebeveiliging en privacy binnen Onderwijsgroep Tilburg en stelt het beleid en de beheer- en beveiligingsmaatregelen op het gebied van informatiebeveiliging en privacy vast. De inhoudelijke verantwoordelijkheid voor informatiebeveiliging is belegd bij de Coördinator Informatiebeveiliging. De inhoudelijke verantwoordelijkheid voor de privacy is belegd bij de Functionaris Gegevensbescherming. Deze hebben de opdracht om voor de informatiebeveiliging en privacy voor de gehele organisatie zorg te dragen.

De voorzitter van het College van Bestuur heeft binnen Onderwijsgroep Tilburg informatiebeveiliging en privacy in zijn portefeuille en is verwerkingsverantwoordelijke, zoals bedoeld in de AVG. Op strategisch niveau is informatiebeveiliging en privacy als beleidsterrein belegd binnen het strategisch informatiemanagement onder verantwoordelijkheid van de strategisch Informatiemanager.

Informatiemanager

Het informatiebeveiligings- en privacy beleid wordt opgesteld door de Informatiemanager (IM) en vastgesteld door het College van Bestuur.

Coördinator Informatiebeveiliging

De Coördinator Informatiebeveiliging (CIB) heeft een rol op tactisch niveau. De CIB adviseert samen met de Informatiemanager (IM) en het Hoofd Operationele Services aan het College van Bestuur. De Coördinator Informatiebeveiliging bewaakt de uniformiteit van beheers- en beveiligingsmaatregelen binnen de organisatie.

Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming (FG) houdt binnen Onderwijsgroep Tilburg toezicht op de toepassing en naleving van de relevante privacywetgeving, zoals AVG. De wettelijke taken en bevoegdheden van de Functionaris Gegevensbescherming geven de FG een onafhankelijke toezichthoudende positie en rol binnen de organisatie.

Coördinator Functioneel Beheer

De Coördinator Functioneel Beheer (CFB) coördineert het functioneel beheer van de onderwijs- of bedrijfsapplicaties en heeft een rol op tactisch niveau. De CFB vervult een rol bij de vertaling van de tactische naar operationele plannen voor de functioneel beheerders. Dit doet de CFB samen met de Coördinator Informatiebeveiliging (vanwege de uniformiteit) en met de eigenaren van de applicaties en technische platforms.

De Architect Technische Infrastructuur

De Architect Technische Infrastructuur adviseert over specifieke informatiebeveiligingsmaatregelen binnen de technische infrastructuur (bijvoorbeeld het netwerk, de gegevensopslag en identiteitenbeheer).

Proceseigenaar

Een proceseigenaar is iemand die verantwoordelijk is voor een van de onderwijs of ondersteunende processen. Deze processen dienen te voldoen aan de informatiebeveiligingskaders die door Onderwijsgroep Tilburg zijn vastgesteld.

Systeemeigenaar

De systeemeigenaar is er verantwoordelijk voor dat de applicatie een goede ondersteuning biedt aan het proces. 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 proceseigenaar, de gebruikers zelf en aan wet- en regelgeving. Uiteraard moet de applicatie voldoen aan het IBP-beleid en tenminste aan de beveiligingsmaatregelen.

Hoofd Operationele Services

Het Hoofd Operationele Services is verantwoordelijk voor het alloceren van middelen om de vastgestelde maatregelen te realiseren.

Leidinggevende

Naleving van het informatiebeveiligings- en privacy beleid is onderdeel van de integrale bedrijfsvoering en de verantwoordelijkheid van de schooldirecteuren en hoofden. Iedere leidinggevende heeft de volgende taken:

- Toezien op de naleving van het IBP-beleid door hun medewerkers;
- Zorgen dat hun medewerkers voldoende geschoold zijn in het kader van privacy, AVG en IBP;
- Zorgen dat hun medewerkers op de hoogte zijn van de beveiligingsmaatregelen;
- Vastleggen van de taken en rollen van hun medewerkers en de daarbij behorende rechten binnen de betreffende systemen en processen;

Leidinggevenden hebben bovendien de volgende taken:

- Toetsen dat er geen gegevens door externe verwerkers worden verwerkt of aan externe partijen worden overgedragen zonder wettelijke grondslag en een geldige overeenkomst (contract en verwerkers-overeenkomst); en
- Beoordelen van incidenten rondom persoonsgegevens en het intern melden daarvan las het vermoeden bestaat dat het gaat om een datalek.

3.2 Overleggen

Om de samenhang in de rollen en verantwoordelijkheden goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van informatiebeveiliging en privacy op elkaar af te stemmen wordt bij Onderwijsgroep Tilburg op meerdere niveaus gestructureerd overleg gevoerd over het brede onderwerp informatiebeveiliging en privacy.

Op strategisch niveau wordt richtinggevend en adviserend gesproken over informatiebeveiliging en privacy in de Overleggroep Bedrijfsvoering (tactisch/strategisch). Informatiebeveiliging en privacy maken onderdeel uit van de A3 Informatie en Technologie in het Meerjarenbeleidsplan van Onderwijsgroep Tilburg. De IM is verantwoordelijk voor het strategisch informatiemanagement en het onderdeel IBP daarbinnen en agendeert dit bij de Overleggroep Bedrijfsvoering.

Op tactisch niveau wordt de strategie vertaald naar tactische en operationele plannen, te hanteren normen, standaarden, toetsingskaders e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg is centraal georganiseerd in het Architectenplatform (AP).

De functionarissen op het gebied van informatiebeveiliging en privacy monitoren de toepassing en naleving van het IBP-beleid. De uitvoering van het jaarlijks actieplan IBP is belegd bij het IBP-team. Dit IBP-team is verantwoordelijk voor het (laten) uitvoeren en het realiseren van het plan. Het IBP-team bestaat uit de Informatiemanager, Coördinator Informatiebeveiliging en Functionaris Gegevensbescherming en - op afroep - een juriste met privacy als aandachtsgebied.

Bovengenoemde functionarissen werken samen met de Architect Technische Infrastructuur en Inkoop in het Inkoop Advies Overleg. Doel van dit overleg is leidinggevenden te adviseren en ondersteunen bij bijvoorbeeld het afsluiten van overeenkomsten met ICT- en applicatie-leveranciers. De leidinggevende wordt ondersteund en geadviseerd over alle technische, functionele, juridische, informatiebeveiligings- en privacy aspecten bij de inkoop van digitale leermiddelen, licenties, applicaties e.d. De Afdeling Inkoop is hiervoor het centraal aanspreekpunt voor de leidinggevende.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm is decentraal georganiseerd. Voor alle drie de typen overleg geldt dat het zoveel mogelijk ingepast wordt in bestaande overlegvormen. Zo zal op strategisch niveau niet alleen over informatiebeveiliging en privacy gesproken worden, maar ook over andere risico’s waarmee de organisatie te maken kan krijgen, zoals bijvoorbeeld financieel en continuïteit.

In het geval van een beveiligingscalamiteit of datalek wordt een Incident Response Team (IRT) gevormd en aangesloten bij de bestaande structuur voor crisismanagement. Het IRT bestaat uit het Hoofd Operationele Services, de IM, de FG, de CIB en op afroep een juriste.

4 Bijlage

Diverse aanvullende beleidsstukken, reglementen, gedragscodes en procedures geven invulling aan de uitwerking van het IBP-beleid. Deze bijlage geeft een (niet-limitatief) overzicht van de diverse aanvullende documenten. Het overzicht is gegroepeerd op de categorieën informatiebeveiliging en privacy. Voor de aanvullende documenten wordt gebruik gemaakt van de IBP-documenten uit het Framework IBP in het MBO van saMBO-ICT en de Aanpak IBP in het VO van Kennisnet.

Informatiebeveiliging

- IAA-Beleid (Identificatie, Authenticatie en Autorisatiebeleid)
- Classificatiemodel
- Bewaartermijnen conform Documentair Structuurplan (DSP)
- Lidmaatschap IM- en IBP-netwerken
- Clear desk, clear screen
- ICT Gedragscode
- BYOD / CYOD Beleid
- Wachtwoordbeleid
- Toegangsbeveiliging
- Logging

Privacy

- Procedure toestemming gebruik beeldmateriaal (toestemmingsverklaring)
- Procedure voor verwijderen van gegevens (bewaartermijnen)
- Communicatie rechten betrokkenen (privacystatement)
- Privacyreglementen (medewerkers, studenten en leerlingen)
- Procesbeschrijving melden datalekken
- Dataregisters
- Verwerkersovereenkomsten
- Procedure Data Protection Impact Assessment (DPIA)