Model informatiebeveiligings- en privacy beleid voor de mbo sector

(op basis van ISO27001/2 en AVG)

IBPDOC6

GEBRUIKERSGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Verantwoording

Bron:

Starterkit Informatiebeveiliging
Stichting SURF
Februari 2015

Bewerkt door:

Kennisnet / saMBO-ICT

Auteurs

Casper Schutte (ROC Midden Nederland)
Ludo Cuijpers (saMBO-ICT)
Leo Bakker (Kennisnet)
Job Vos (Kennisnet)

Versie 2.0, juli 2016

Sommige rechten voorbehouden

Inhoudsopgave

1. Inleiding

1.1 Toelichting informatiebeveiliging beleid

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[1].

Informatiebeveiliging is een beleidsverantwoordelijkheid van het bestuur van **<naam mbo instelling>**. 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 nemen. Immers, onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

<Naam mbo instelling> 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 Toelichting privacy beleid

Het privacy beleid heeft betrekking op het verwerken van Persoonsgegevens van alle Betrokkenen binnen **<naam mbo instelling>** waaronder in ieder geval alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur/outsourcing), evenals op andere Betrokkenen waarvan **<naam mbo instelling>** Persoonsgegevens verwerkt.

In het Beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van Persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van **<naam mbo instelling>** 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 **<naam mbo instelling>** 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 **<naam mbo instelling>** heeft tot 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 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 **<naam mbo instelling>.**

[1] Zie bijlage 1 voor toelichting.

1.3 Vervlechting informatiebeveiliging <naam mbo instelling> en privacy (ibp)

In de reikwijdte van het beleid wordt beschreven wat de afbakening is van het toepassingsgebied ervan. Bij **<naam mbo instelling>** wordt informatiebeveiliging (processen) gekoppeld aan Privacy (mensen). Het informatiebeveiligings- en privacy beleid binnen **<naam mbo instelling>** heeft betrekking op alle medewerkers, studenten, gasten, geregistreerde bezoekers en externe relaties (inhuur / outsourcing), alsmede op alle organisatieonderdelen. 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 **<naam mbo instelling>.** Dit heeft zowel betrekking op *gecontroleerde informatie*, die door de instelling zelf is gegenereerd en wordt beheerd, als ook op *niet-gecontroleerde informatie*, bijv. uitspraken van studenten in discussies, persoonlijke websites op zakelijke personal pages, waarop de instelling kan worden aangesproken.

1.4 Doelstelling informatiebeveiligings- en privacy beleid

Het informatiebeveiligings- en privacy beleid bij **<naam mbo instelling>** 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 en het minimaliseren van eventuele gevolgen.

Het doel van het informatiebeveiligings- en privacy beleid voor **<naam mbo instelling>** is concreet het volgende:

Kader: het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging en privacy 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) en privacy wetgeving.

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

Expliciet: uitgangspunten en organisatie van informatiebeveiliging 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 de beleidsmaatregelen.

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

Door het concretiseren van informatiebeveiligings- en privacy beleid op procesniveau van **<naam mbo instelling>** wordt aantoonbaar dat dit beleid bijdraagt aan de realisering van de overall doelstellingen die **<naam mbo instelling>** voor zichzelf heeft geformuleerd *('alignment').* Die doelstellingen zijn het bieden van een kwalitatief hoogwaardige onderwijsomgeving, dat 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 (Privacy) is noodzakelijk om te voldoen aan wettelijk voorgeschreven uitwisselingen van gegevens en voor de bedrijfsprocessen van instellingen van onderwijs. Dit dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van Persoonsgegevens grote schade kan berokkenen aan studenten, medewerkers en andere Betrokkenen bij **<naam mbo instelling>**, maar ook bij **<naam mbo instelling>** zelf. **<Naam mbo instelling>** 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 **<naam mbo instelling>**.

Met het beschrijven van de maatregelen in dit beleidsdocument beoogt en neemt **<naam mbo instelling>** haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van Persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacy wet- en regelgeving.

Het is van belang om het door **<naam mbo instelling>** gevoerde informatiebeveiligings- en privacy beleid ook bekend te maken aan studenten en medewerkers, alsmede om de visie daarover breed uit te dragen. Hiervoor is het gebruik van een privacy reglement (soms ook wel privacy statement genoemd) een goed middel. Dit document beschrijft op welke wijze **<naam mbo instelling>** omgaat met persoonsgegevens van studenten en medewerkers, en wat ieders rechten en verplichtingen zijn. Alhoewel het gebruik van een privacy reglement niet wettelijk is voorgeschreven, is dit toch als bijlage toegevoegd. Dit regelement is evenals het beleidsplan vastgesteld door het CvB en voorzien van instemming van de ondernemingsraad.

2. Beleidsuitgangspunten en -principes informatiebeveiliging en privacy

2.1 Beleidsuitgangspunten informatiebeveiliging en privacy

Informatiebeveiligings- en privacy 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). Hierin worden jaarplannen opgesteld en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen.
Het belangrijkste beleidsuitgangspunt bij **<naam mbo instelling>** is:

- Onze filosofie is dat we een open, transparante en toegankelijke instelling zijn.

Dit open en toegankelijk karakter heeft betrekking op gasten, maar ook voor studenten 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 studenten 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 (2016).
Hierbij dient een goede balans te worden aangebracht tussen het belang van **<naam mbo instelling>** 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 **<Naam mbo instelling>** 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, studenten, 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 studenten 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. 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:

- Een Verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd in artikel 8 van de Wet bescherming persoonsgegevens (Wbp).
- Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de Verwerking geformuleerd.
- Bij een 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.
- Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde.
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen.
- Persoonsgegevens worden niet *verder* verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
- 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.
- 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[2] procedure worden aangeboden

[2] Zie AVG

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 je als instelling loopt bij de verwerking van deze gegevens zo klein mogelijk maakt.

3.1 Risico's

De proceseigenaren van **<naam mbo instelling>** 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:
(hieronder een opsomming van de prioriteiten met betrekking tot mitigatie van risico's binnen de instelling, een *voorbeeld* set zou kunnen zijn:)

- 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

<naam mbo instelling> hanteren de classificatie standaarden zoals die verwoord zijn in Certificeringsschema Informatiebeveiliging en privacy dat wordt beheerd binnen Edustandaard. Deze standaard is onderdeel van de Referentie Onderwijs Sector Architectuur (ROSA).[3]

Bij **<naam mbo instelling>** zijn 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 gekozen:

Classificatie indeling	Classificatie gevolg	Beheersmaatregel
Beschikbaarheid **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, haar medewerkers of haar studenten of klanten.	Zie: Certificeringsschema Informatiebeveiliging en privacy

B. Integriteit
Voor integriteit wordt de volgende classificatie indeling gehanteerd:

Classificatie indeling	Classificatie gevolg	Beheersmaatregel
Integriteit **Laag**	Het bedrijfsproces staat **enkele** integriteitsfouten toe.	Applicatie controle
Integriteit **Midden**	Het bedrijfsproces staat **zeer weinig** integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk.	Applicatie plus menselijke controle

[3] Een initiatief van Kennisnet.

Integriteit **Hoog**	Het bedrijfsproces staat **geen** integriteitsfouten toe.	Applicatie plus twee maal menselijke controle

C. Vertrouwelijkheid
Vertrouwelijkheid is als volgt geclassificeerd:

Classificatie indeling	Classificatie gevolg	Beheersmaatregel
Vertrouwelijkheid **Laag**	Informatie die toegankelijk mag of moet zijn voor **alle of grote groepen** medewerkers of ouders of leerlingen. Vertrouwelijkheid is gering.	Toegang tot network op basis van arbeidsovereenkomst of leerling inschrijving.
Vertrouwelijkheid **Midden**	Informatie die alleen toegankelijk mag zijn voor een **beperkte groep** gebruikers. De informatie is vertrouwelijk.	Toegang op basis van autorisatiematrix
Vertrouwelijkheid **Hoog**	Dit betreft zeer vertrouwelijke informatie, alleen bedoeld voor **specifiek benoemde personen**, waarbij onbedoeld bekend worden buiten deze groep grote schade kan toe brengen.	Toegang op basis van autorisatiematrix plus pasje of sms code (2 way authentication)

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.

3.3 Voorbeeld classificatie en labelen

Deze classificatie wordt samengevat tot BIV (Beschikbaarheid-Integriteit-Vertrouwelijkheid) waar vervolgens door de proceseigenaren scores aan worden toegevoegd. 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 **<naam mbo instelling>** wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

4.1.1 Wet Educatie en Beroepsonderwijs (WEB)

<Naam mbo instelling> heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studenten administratie en met de studieresultaten is gewaarborgd..

4.1.2 Algemene Verordening Gegevensbescherming (AVG)

<Naam mbo instelling> heeft de wettelijke vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) geïmplementeerd via het informatiebeveiligings- en privacy beleid.
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

<Naam mbo instelling> 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

<Naam mbo instelling> verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat **<naam mbo instelling>** 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 **<naam mbo instelling>** 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 **<naam mbo instelling>** gebaseerd op ISO 27001.
<Naam mbo instelling> 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) van **<Naam mbo instelling>**. Dit is een formele aanvulling op de arbeidsovereenkomst.

5. Governance informatiebeveiligingsbeleid

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, studenten, 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 **<naam mbo instelling>** op strategisch niveau zowel aandacht geschonken wordt aan informatiebeveiligings- en privacy beleid, als aan 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 en privacy daarin.

5.2 Inpassing ibp governance in <naam mbo instelling>

In deze paragraaf wordt beschreven hoe ibp-governance in **<naam mbo instelling>** 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 operationeel niveau. Hij adviseert samen met de directeur it en/of de Informatiemanager aan het College van Bestuur. De manager ibp bewaakt de uniformiteit binnen de instelling.
Op operationeel niveau wordt overlegd met de functionele (functioneel beheer Financiën en functionele beheerders van bijvoorbeeld educatieve applicaties) en technische beheerders. Er wordt aandacht geschonken aan de implementatie van de informatiebeveiliging en privacy maatregelen.

Schematisch weergegeven:

Niveau	*Wat?*	*Wie?*	*Overleg*	*Documenten*
Richtinggevend	• *Bepalen ibp strategie* • *Organisatie t.b.v. ibp inrichten* • *ibp-planning en control vaststellen* • *Business continuity management*	• *CvB, i.c Portefeuillehouder IB, o.b.v. advies manager ibp* • *Directeur Onderwijs* • *Directeur HR* • *Directie ICT*	*CvB stelt vast Strategisch ibp- overleg adviseert*	• *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 eigenaren* • *manager ibp* • *Functionele beheerders* • *Functionaris voor de Gegevensbescherming*	*Tactisch ibp overleg*	• *Risicoanalyses en audits* • *Jaarplan en verslag*
Uitvoerend	• *Implementeren ibp-maatregelen* • *registreren en evalueren incidenten* • *communicatie eindgebruikers*	• *Functioneel Beheerder* • *ICT*	*Operationeel ibp overleg*	• *SLA's (security paragraaf)* • *Incident registratie, incl. evaluatie*

De financiering van informatiebeveiliging en privacy wordt bij **<naam mbo instelling>** als volgt geregeld. Algemene zaken, zoals het opstellen van een informatiebeveiliging en privacy plan voor de gehele instelling of een externe audit, worden uit het centrale ibp-budget betaald. De beveiliging van informatiesystemen komen 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 en privacy

Voor informatiebeveiliging en privacy wordt bij **<naam mbo instelling>** dezelfde managementcyclus gevolgd, die ook voor andere onderwerpen geldt: beleid, analyse, plan implementatie, uitvoering, controles en evaluatie.

5.3.1 Het informatiebeveiligings- en privacy beleid

Het informatiebeveiligings- en privacy beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen de instelling. In het informatiebeveiligings- en privacy 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 informatiebeveiligings- 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 (baseline) 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 manager ibp[4], in samenwerking met de proceseigenaren, de directeur ICT, de informatiemanager en de directeur Financiën.

5.3.5 Diensten niveau overeenkomsten (DNO’n of 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 informatiebeveiliging en privacy paragraaf, waarin de verantwoordelijkheden van de leverancier zijn opgenomen.

[4] Dit kan uiteraard ook belegd worden bij andere functionarissen.

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 het sluiten van bewerkersovereenkomsten of overeenkomen van geheimhoudingsbedingen. Hetzelfde is van belang bij uitbestedingen.

5.3.8 Policies[5]

Gedragscodes en richtlijnen voor medewerkers, studenten en derden, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging en privacy.

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 **<naam mbo instelling>** initieert de manager ibp in samenwerking met de interne auditor de controle op de uitvoering van het informatiebeveiliging en privacy 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 **MBOaudit** (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 **<naam mbo instelling>.**
De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het informatiebeveiliging en privacy proces. Van belang hierbij is dat lijnmanagers en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Voor de bevordering van de naleving van de Wet Bescherming Persoonsgegevens vervult de functionaris gegevensbescherming (FG) een belangrijke rol, bijvoorbeeld ten aanzien van opname en afhandeling van klachten. Deze wordt ingesteld door het College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. Deze FG werkt via een door het CvB vast te stellen reglement. Mocht de naleving ernstig tekort schieten, dan kan **<naam mbo instelling>** de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Naast of in plaats van het instellen van een FG, kan de instelling er voor kiezen om een privacy officer aan te stellen. Deze medewerker heeft privacy in zijn of haar portefeuille. Anders dan de FG, zal de privacy officer meer in de uitvoering betrokken zijn en minder een toezichthoudende rol hebben. Optie: **<naam mbo instelling>** heeft de rol van FG belegd bij de jurist of de vertrouwenspersoon van de instelling.

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 **<naam mbo instelling>**

[5] Voor een aantal van deze policies is gebruik gemaakt van documenten uit mbo framework ibp IBPDOC6, versie 2.0, **Model op basis van ISO27001/2 en AVG**

het bewustzijn voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en het (veilig en verantwoord) gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, deelnemers 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 beveiligingsbewustzijn is een verantwoordelijkheid van de manager ibp; uiteindelijk is ook hiervoor het College van Bestuur eindverantwoordelijk.

5.6 Organisatie van de informatiebeveiliging en privacy rollen (functies)

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij **<naam mbo instelling>** een aantal rollen onderkend die aan functionarissen in de bestaande organisatie zijn toegewezen.

College van Bestuur
Het College van Bestuur is eindverantwoordelijk voor de informatiebeveiliging en privacy binnen **<naam mbo instelling>** en stelt het beleid en de basis maatregelen op het gebied van informatiebeveiliging en privacy vast. De inhoudelijke verantwoordelijkheid voor informatiebeveiliging en privacy is gemandateerd aan de ibp manager. Deze heeft de opdracht om voor de informatiebeveiliging en privacy voor de gehele instelling zorg te dragen.

Portefeuillehouder informatiebeveiliging
Het Collegelid dat informatiebeveiliging en privacy in zijn portefeuille heeft is eindverantwoordelijk voor informatiebeveiliging en privacy binnen **<naam mbo instelling>.**

Manager ibp
De manager ibp is een rol op strategische en tactisch/operationeel niveau. Hij adviseert samen met de directeur ICT en Informatiemanager aan het College van Bestuur. De manager ibp bewaakt de uniformiteit binnen de instelling.

Functioneel beheerder
De rol van functioneel beheerder onderwijs- of bedrijfsapplicatie is vormgegeven op het stafniveau van elke organisatorisch onderdeel. Deze vervult een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit doen ze samen met de ibp manager en met de eigenaren van de technische platforms.

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

Systeemeigenaar
De systeemeigenaar is er verantwoordelijk voor dat de 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 informatiebeveiligingsbeleid en tenminste aan de basis maatregelen.

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

Leidinggevende
Naleving van het informatiebeveiligingsbeleid 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 beveiliging en privacy beleid;
- toe te zien op de naleving van het beveiliging en privacy 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 informatiebeveiliging en privacy zaken.

De leidinggevende kan hierin ondersteund worden door de manager ibp.

Functionaris Gegevensbescherming[6]
De functionaris voor de gegevensbescherming (FG) houdt binnen **<naam mbo instelling>** 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 (optie is een privacy officer).

CERT-coördinator
De CERT-coördinator bij **<naam mbo instelling>** wordt benoemd door de directeur ICT op instellingsniveau en opereert in diens opdracht. Hij is bevoegd het isoleren van computersystemen of netwerksegmenten te gelasten. De coördinator is tevens de contactpersoon voor SURFnet.

5.7 Overleg

Om de samenhang in de organisatie van de informatiebeveiliging en privacy functie goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van informatiebeveiliging en privacy binnen de verschillende onderdelen op elkaar af te stemmen wordt bij **<naam mbo instelling>** gestructureerd overleg gevoerd over het onderwerp informatiebeveiliging en privacy 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, bijvoorbeeld, in het strategisch ICT-overleg.

Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg is per sector, portaal of dienst georganiseerd.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm is zeer decentraal georganiseerd, indien nodig in elk organisatieonderdeel. 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 en privacy gesproken worden, maar ook over andere risico's waarmee de instelling te maken kan krijgen, zoals bijvoorbeeld financieel, personeel en continuïteit.

[6] Zie IBPDOC12 Competenties Informatiebeveiliging en Privacy, pagina 21

6. Melding en afhandeling van incidenten

6.1 Registratie informatiebeveiliging en privacy incidenten

Incidentbeheer en –registratie hebben betrekking op de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging en privacy door de medewerkers en studenten 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 **<naam mbo instelling>** is er daarom een Meldpunt[7] ingericht en is bekend gemaakt hoe dat is te benaderen.
De lijnmanager dient de incidenten en inbreuken direct te melden aan het Meldpunt **<naam mbo instelling>**.
Gezien de meldplicht datalekken die per 1 januari 2016 is opgenomen in de WBP heeft **<naam mbo instelling>** een protocol datalekken ontwikkeld. Daarin is beschreven op welke wijze binnen 2 werkdagen bij de toezichthouder datalekken kunnen worden gemeld. 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. Deze korte meldingstermijn maakt dat vooraf procesafspraken in een datalekken protocol zijn gemaakt en dat er een medewerker (de FG of privacy officer) is aangewezen om deze melding te doen. De privacy-toezichthouder College Bescherming Persoonsgegevens maakt in ene richtsnoer in december 2015 bekend op welke manieren een datalek moet worden gemeld.

6.2 Informatiebeveiliging en Privacy Crisis Team (IPCT)

Het doel van het Informatiebeveiliging en Privacy Crisis Team (IPCT) bij **<naam mbo instelling>** is instelling brede preventie en curatieve zorg voor informatiebeveiliging en privacy incidenten. Het IPCT houdt zich ook bezig met beveiligingsincidenten buiten **<naam mbo instelling>** als daar eigen medewerkers of deelnemers in enige rol bij betrokken zijn.
Optie: In zulke gevallen wordt in principe gebruik gemaakt 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 Besturen en opereren in diens opdracht. Het IPCT is gerechtigd het isoleren van computersystemen of netwerksegmenten te gelasten.
Het IPCT van **<naam mbo instelling>** heeft de volgende opdracht:

- Het signaleren en registreren[8] 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 aan directeur ICT, directeur HR en de Informatiemanager over de beveiligingsincidenten en het doen van voorstellen tot betere preventie van of curatie op incidenten.

Het IPCT bij **<naam mbo instelling>** levert de volgende diensten bij calamiteiten:

- 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.
- De bereikbaarheid van de IPCT (tijden/middelen) worden bekend gemaakt 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;
- Optie: Onderhoudt contacten met SURFcert (indien aangesloten bij SURF).

[7] Meldpunt ook wel helpdesk of servicepunt genoemd. Registratie kan plaatsvinden in (bijvoorbeeld) Topdesk.
[8] Bijvoorbeeld m.b.v. Topdesk

Het IPCT bij **<naam mbo instelling>** behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.
De dienstverlening van het IPCT bij **<naam mbo instelling>** is gedocumenteerd en door het College van Bestuur bekrachtigd. De rol van IPCT coördinator kan het beste worden belegd bij de ibp manager.

Bijlage 1: Toelichting 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.


Voorbeeld classificatie model.do

Bijlage 2: Gerelateerde documenten (niet opnemen in ibp plan)

Privacy reglementen Onderwijs Gemeenschap Tilburg

Privacyreglementen deelnemers en personeel OGT (PDF 245 kB)

Privacy reglement deelnemers OGT (PDF 322 kB)

Privacyreglement personeel OGT (PDF 415 kB)

Kennisnet

Privacy in 10 stappen (PDF 2003 kB)

Vijf vuistregels voor privacy (PDF 93 kB)

Voorbeeldteksten transparantie over privacy (DOC 32 kB)

Stappenplan datalekken

De meldplicht datalekken in de Wet bescherming persoonsgegevens (PDF 1180 kB)

Meldplicht datalekken (PDF 187 kB)

Bijlage 3: Framework informatiebeveiliging en privacy in het mbo