ONDERWIJSGROEP TILBURG

Informatiebeveiligings- en Privacybeleid
Onderwijsgroep Tilburg
op basis van ISO27001 en ISO27002

Versie:	1.1
Status:	Definitief
Datum:	16 oktober 2018
Datum vaststelling CvB: 26 november 2018	

Versiebeheer

Versienr.	Datum	Auteur(s)	Status	Opmerking
0.1	03-03-2015	B. Bogers	Concept	Voor commentaar
0.2	17-11-2015	B. Bogers	Concept	Review F. van Dijk /Joel de Bruijn
0.3	05-12-2015	B. Bogers	Concept	Review Hans Hermans
0.4	13-06-2016	B. Bogers	Vaststelling	Review Hans Hermans Privacy aanpassing
0.5	Na de herfstva-kantie	B. Bogers	Review	Staf review t.b.v. vaststelling
0.6	10-07-2017	B.Bogers/Niels Dutij	Goedkeuring SPIM	Aanpassingen i.v.m. aanstelling Functionaris gegevensbescherming
0.7	06-11-2017	N.Dutij	Operationeel overleg	Voorleggen ter goedkeuring
1.0	09-01-2018	N. Dutij	Vaststelling	
1.1	16-10-2018	J. de Bruijn	Concept	Aanpassing paragraaf 5.3.7 in verband met eisen aan leveranciers tijdens inkoop.
1.1	26-10-2018	J. de Bruijn	Vaststelling	CvB/1718.038a

Verantwoording

Bron:

Starterkit Informatiebeveiliging
Stichting SURF
Februari 2015

Bewerkt door:

Bram Bogers CISM Onderwijsgroep Tilburg

Sommige rechten voorbehouden

Inhoudsopgave

Inhoud

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 de Onderwijsgroep Tilburg. 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.

Onderwijsgroep Tilburg heeft de ambitie om met het onderhavige beleidsdocument informatiebeveiliging en privacy 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 informatie- en privacy beveiligingsbeleid (IBP) ook in hun onderlinge relatie duidelijk te beschrijven en vast te stellen.

De kwaliteitsaspecten:

Beschikbaarheid:	de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers;
Integriteit:	de mate waarin gegevens of functionaliteit juist ingevuld zijn;
Vertrouwelijkheid:	de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

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

1.2 Toelichting privacy beleid

Het privacy beleid heeft betrekking op het verwerken van Persoonsgegevens van alle Betrokkenen binnen de Onderwijsgroep Tilburg waaronder in ieder geval alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur/outsourcing), evenals op andere Betrokkenen waarvan de Onderwijsgroep Tilburg Persoonsgegevens verwerkt.

In het Beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van Persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van de Onderwijsgroep Tilburg 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 de Onderwijsgroep Tilburg 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 de Onderwijsgroep Tilburg 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

[1] Zie bijlage 1 voor toelichting.

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 de Onderwijsgroep Tilburg.

1.3 Vervlechting informatiebeveiliging en privacy (ibp)

In de reikwijdte van het beleid wordt beschreven wat de afbakening is van het toepassingsgebied ervan. Bij de Onderwijsgroep Tilburg wordt informatiebeveiliging (processen) gekoppeld aan Privacy (mensen). Het informatiebeveiligings- en privacy beleid binnen de Onderwijsgroep Tilburg 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 de 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*, 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 de Onderwijsgroep Tilburg 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 de Onderwijsgroep Tilburg 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 de Onderwijsgroep Tilburg wordt aantoonbaar dat dit beleid bijdraagt aan de realisering van de overall doelstellingen die de Onderwijsgroep Tilburg 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.

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 de Onderwijsgroep Tilburg, maar ook bij de Onderwijsgroep Tilburg zelf. De Onderwijsgroep Tilburg 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 de Onderwijsgroep Tilburg.

Met het beschrijven van de maatregelen in dit beleidsdocument beoogt en neemt de Onderwijsgroep Tilburg 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 de Onderwijsgroep Tilburg 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) een goed middel. Dit document beschrijft op welke wijze de Onderwijsgroep Tilburg 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.

1.6 Reikwijdte van het beleid

In de reikwijdte van het beleid wordt beschreven wat de afbakening is van het toepassingsgebied ervan. Bij de Onderwijsgroep Tilburg wordt informatiebeveiliging breed geïnterpreteerd. Onderwijsgroep Tilburg realiseert zich dat er een belangrijke relatie en een gedeeltelijke overlap ligt met aanpalende beleidsterreinen, met name ten aanzien van Privacy. Maar ook met beleidsterreinen zoals ARBO- en milieuwetgeving, fysieke beveiliging en business continuity. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht (zie ook hoofdstuk 4).
Het informatiebeveiligingsbeleid binnen de Onderwijsgroep Tilburg heeft betrekking op alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur / outsourcing), alsmede op alle organisatieonderdelen. Tevens vallen onder het informatiebeveiligingsbeleid alle devices van waaraf geautoriseerde toegang tot het instellingsnetwerk verkregen kan worden.
Bij het informatiebeveiligingsbeleid ligt de nadruk op die toepassingen die vallen onder de verantwoordelijkheid van de 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*, bijv. uitspraken van studenten in discussies, persoonlijke websites op zakelijke en persoonlijke pagina's, waarop de instelling kan worden aangesproken.

2 Beleidsuitgangspunten en -principes informatiebeveiliging en privacy

2.1 Beleidsuitgangspunten informatiebeveiliging en privacy

Informatiebeveiligingsbeleid 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.
De beleidsuitgangspunten bij Onderwijsgroep Tilburg zijn:

- Onze filosofie is dat we een open 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 de Onderwijsgroep Tilburg om Persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn Persoonsgegevens.
- De informatiebeveiliging dient bij te dragen aan het waarborgen van de volgende kwaliteitsaspecten van informatievoorziening :
  a. Beschikbaarheid
  b. Integriteit
  c. Vertrouwelijkheid.

Onderwijsgroep Tilburg hanteert de volgende beleidsprincipes:

- Informatiebeveiliging en privacy is een lijnverantwoordelijkheid: dat betekent dat de lijnmanagers (College van bestuur, schooldirecteuren en afdelingshoofden etc.) de primaire verantwoordelijk dragen voor een goede informatiebeveiliging 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.
- Lijnverantwoordelijkheden die middels toegangsbeperkende maatregelen (zoals inloggevens of sleutel) zijn afgeschermd, mogen uitsluitend gedelegeerd worden op basis van eigen autorisatie, de medewerker krijgt door middel van delegatie de lijnverantwoordelijkheid toegewezen (gedelegeerde bevoegde). Het is dan ook niet toegestaan toegangsbeperkende maatregelen door te geven (zoals verstrekken van eigen inloggegevens aan een ander). Op verzoek van de lijnverantwoordelijke aan applicatiebeheer c.q. beheerder van de beperkende middelen kunnen persoonsgebonden toegangsbeperkende maatregelen ter beschikking worden gesteld aan de medewerker aan wie de lijnverantwoordelijke de bevoegdheden wenst te delegeren.
- 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 instellings-brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
- Informatiebeveiliging is 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 op efficiency (controleerbaarheid).

- Eigendom van informatie: de onderwijsinstelling is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd, tenzij dit voor bijvoorbeeld een externe opdracht onderzoek anders is overeengekomen. 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 hij de informatie middels een informatiesysteem (applicatie) en ziet toe op juiste classificatie, middels risicoanalyse, 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.
- Classificatie van informatie: iedereen behoort de classificatie van informatie te kennen en daarnaar te handelen. Deze classificatie wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid. Zie paragraaf 3, Classificatie.
- Bij projecten, zoals infrastructurele wijzigingen, de aanschaf van nieuwe systemen of wijzigingen van bestaande systemen dient vanaf de start rekening gehouden te worden met informatiebeveiliging.

2.2 Privacy principes

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

- Een Verwerking van Persoonsgegevens is gebaseerd op een wettelijke grondslag.
- 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 kenbaar worden gemaakt dat hij zijn toestemming altijd kan intrekken.

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 de Onderwijsgroep Tilburg 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 Classificatie en gehanteerde standaard

De Onderwijsgroep Tilburg 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).[2]

Bij Onderwijsgroep Tilburg 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
- Integriteit
- Vertrouwelijkheid.

Ten aanzien van de beschikbaarheidseisen worden de volgende klassen onderscheiden:

Klasse	Basisprincipes
Niet vitaal	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, haar medewerkers of haar klanten.
Vitaal	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar klanten.
Zeer vitaal	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 etmaal brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar klanten.

Voor integriteit wordt de volgende indeling gevolgd:

[2] Een initiatief van Kennisnet.

integriteitsklasse	Basisprincipes
Geen gevolgen	Dit is het basisniveau. Wanneer de data onjuist, onvolledig of niet op tijd is, dan gaat het proces gewoon door en zal de kwaliteit van het proces op gelijke hoogte blijven.
Enige schade	Wanneer de data onjuist, onvolledig en niet op tijd is, dan zal dit het proces hinderen, maar het zal door blijven lopen. Schade kan ontstaan maar dit is kleine schade, bijvoorbeeld in de vorm van verlies van productie of het moeten overdoen van handelingen. Bij de student of medewerker zal geen schade ontstaan. Er zijn geen gerechtelijke- of financiële consequenties voor Onderwijsgroep Tilburg
Veel schade	De data is zodanig vervuild of beschadigd en zodanig cruciaal dat dit ernstige gevolgen voor het proces heeft. Er kunnen fouten gemaakt zijn, die grote schade veroorzaakt hebben bij Onderwijsgroep Tilburg. Het proces moet stilgelegd worden om verdere schade te beperken. Schade of foutieve conclusies kunnen plaatsvinden die financiële, gerechtelijke of andere consequenties kunnen hebben voor Onderwijsgroep Tilburg.

Vertrouwelijkheid is ingedeeld in de volgende klassen:

Klasse	Basisprincipes
Openbaar	• Iedereen mag de gegevens inzien, bijvoorbeeld de website van Onderwijsgroep Tilburg • Een geselecteerde groep mag deze gegevens wijzigen
Intern	• Iedereen die aan de instelling is verbonden als medewerker of student mag deze gegevens inzien; toegang kan zowel binnen als buiten de instelling (remote) worden verleend, bijvoorbeeld lesroosters of elektronische leeromgeving • Een geselecteerde groep mag deze gegevens wijzigen.
Vertrouwelijk	• Er is expliciet aangegeven wie welke rechten heeft t.a.v. de raadpleging en de verwerking van deze gegevens, bijvoorbeeld Deelnemersvolgsysteem.

Welk beveiligingsniveau geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt. De classificatie dient door of namens de eigenaar van het betreffende informatiesysteem te worden bepaald. Onderstaande tabel geeft weer welk beveiligingsniveau bij welke klasse van informatie behoort:

Beschikbaarheid	
Niet vitaal	Basisbescherming
Vitaal	Basisbescherming +
Zeer vitaal	Basisbescherming ++
Integriteit	
Geen gevolgen	Basisbescherming
Enige schade	Basisbescherming
Veel schade	Basisbescherming +
Vertrouwelijkheid	
Openbaar	Basisbescherming
Intern	Basisbescherming
Vertrouwelijk	Basisbescherming +

Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen. Met basisbescherming + wordt dus een hoger beveiligingsniveau bedoeld dan bij basisbescherming.

Basisbescherming ++ is het hoogste beschermingsniveau bij Onderwijsgroep Tilburg. Voor de beschrijving en uitwerking van genoemde beschermingsniveaus bestaat een apart document. Onderwijsgroep Tilburg heeft een aparte classificatiemethodiek geformuleerd.

4 Wet- en regelgeving

4.1 Wettelijke voorschriften

Bij de Onderwijsgroep Tilburg wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

4.1.1 Wet Educatie en Beroepsonderwijs (WEB)

De Onderwijsgroep Tilburg 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)

De Onderwijsgroep Tilburg 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

De Onderwijsgroep Tilburg 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

De Onderwijsgroep Tilburg verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat de Onderwijsgroep Tilburg 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 de Onderwijsgroep Tilburg 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 de Onderwijsgroep Tilburg gebaseerd op ISO 27001. De Onderwijsgroep Tilburg 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 de Onderwijsgroep Tilburg. 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 Onderwijsgroep Tilburg 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 in de IBP governance

In deze paragraaf wordt beschreven hoe IBP-governance in Onderwijsgroep Tilburg 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 coördinator informatiebeveiliging is een rol op tactisch niveau. Hij adviseert samen met de Informatiemanager aan het strategisch platform informatiemanagement (SPIM). De coördinator informatiebeveiliging bewaakt de uniformiteit en de uitvoering van het beleid binnen de instelling.

De functionaris gegevensbescherming houdt toezicht op de verwerking van persoonsgegevens. De functionaris gegevensbescherming werkt als onafhankelijke toezichthouder en geeft gevraagd en ongevraagd advies op het gebied van privacy. De functionaris gegevensbescherming adviseert daarom ook aan het SPIM op het gebied van technologie en privacy.

Het architecten platform (AP) vervult een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit doen ze samen met de coördinator informatiebeveiliging (vanwege de uniformiteit) en met de eigenaren van de technische platforms. Op operationeel niveau wordt overlegd onder aansturing van de coördinator functioneel beheer 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 informatiebeveiligingsmaatregelen.

Schematisch weergegeven:

Niveau	*Wat?*	*Verantwoordelijk*	*Betrokken*	*Overleg*	*Documenten*
Richtinggevend	• *Bepalen IBP strategie* • *Organisatie t.b.v. IBP inrichten* • *IB-planning en control vaststellen* • *Business continuity strategie uitdragen van IB beleid (voorbeeldfunctie)*	• *CvB, i.c. Portefeuillehouder Informatiebeveiliging.*	• *SPIM en coördinator informatiebeveiliging vervullen een adviserende rol.* • *Functionaris gegevensbeveiliging.*	*CvB stelt vast SPIM adviseert*	• *IBP beleidsplan* • *IBP baseline (basis maatregelen)* • *Business Continuity beleid*
Sturend	*Planning & Control IBP:* • *voorbereiden* • *normen en wijze van toetsen* • *evalueren beleid en maatregelen* • *begeleiding externe audits*	• *Proces eigenaar*	• *Functionaris gegevensbeveiliging* • *Coördinator informatie beveiliging* • *Taskforce onderwijs en ICT* • *Coördinator functioneel beheerders*	*Tactisch AP overleg met onderwerp IBP*	• *Risicoanalyses en audits* • *Jaarplan en verslag Business Continuity controles*
Uitvoerend	• *Implementeren IBP-maatregelen* • *registreren en evalueren incidenten* • *communicatie eindgebruikers*	• *Leidinggevende*	• *Coördinator Functioneel Beheerder* • *Technisch architect ICT*	*Functioneel beheerders overleg en Service delivery overleg (ICT)*	• *SLA's (security paragraaf)* • *Incident registratie, incl. evaluatie* • *Toetsing contracten m.b.t. uitwijk en DR, DR-plan, werking HA-maatregelen (incl. back-up), etc.* • *Evaluatie HA- en DR-incidenten/calamiteiten (PDCA)* • *Up to date Business Continuity maatregelen*

De financiering van informatiebeveiliging en privacy wordt bij Onderwijsgroep Tilburg als volgt geregeld:

a. Algemene zaken, zoals het opstellen van een informatiebeveiligings en privacy plan voor de gehele instelling uit het budget van SSC betaald.
b. Externe audits worden uit het centrale budget SSC betaald.
c. De beveiliging van informatiesystemen komen ten laste van de eigenaar van het informatiesysteem zelf.
d. Technische beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten.
e. Bewustwordingscampagnes worden centraal gefinancierd en lokale voorlichting en training voor specifieke toepassingen of doelgroepen worden decentraal gefinancierd.

5.3 Documenten informatiebeveiliging

Voor informatiebeveiliging wordt bij Onderwijsgroep Tilburg dezelfde managementcyclus gevolgd, die ook voor andere onderwerpen geldt: beleid, analyse, plan implementatie, uitvoering, controles en evaluatie.

5.3.1 Het informatiebeveiligings- en privacybeleid

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 te kunnen waarborgen. Dit vloeit voort uit het beleid of uit besluiten die door het SPIM (o.b.v. advies architecten platform) zijn voorgelegd aan het college van bestuur (CvB). Deze basismaatregelen dienen dus overal in de instelling genomen te worden. De baseline wordt gemaakt door de coördinator Informatiebeveiliging 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 twee jaar levert de coördinator Informatiebeveiliging i.o.m. de functionaris gegevensbescherming een jaarverslag en een jaarplan voor de volgende 2 jaar aan bij het SPIM. 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 & Verantwoording-cyclus. Waar nodig wordt apart aandacht besteed aan decentrale systemen.

5.3.4 ICT Continuity Plan

ICT Continuity Management is de benaming van het proces dat potentiële bedreigingen voor de ICT dienstverlening identificeert, bepaalt wat de impact op deze dienstverlening van de organisatie is als deze bedreigingen daadwerkelijk manifest worden en welke maatregelen hierin genomen moeten worden. Het product van het ICT continuity plan bestaat uit een samenhangend stelsel van maatregelen, die zowel preventief, detectief, repressief als correctief werkzaam zijn. Het ICT Continuity Plan wordt opgesteld door het hoofd ICT.

5.3.5 Diensten niveau overeenkomsten (DNO'n of SLA's)

Een servicelevel 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.

5.3.6 Contracten applicaties en educatieve software

De wetgeving verplicht Onderwijsgroep Tilburg om bewerkersovereenkomsten af te sluiten met 'bewerkers'. Bewerkers zijn externe leveranciers die op enige manier toegang of beschikking hebben tot persoonsgegevens van Onderwijsgroep Tilburg. Met bewerkers van onderwijs- en bedrijfsapplicaties en educatieve software worden daarom 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-, 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 verwerkersovereenkomsten 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.

5.3.8 Policies

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

- Reglement Verantwoord Netwerkgebruik, voor het veilig gebruik van ICT-voorzieningen
  Onderdelen hiervan zijn o.a.
    - Gebruik van social media
    - Gebruik van internet
    - Gebruik van e-mail en andere ICT-communicatiemiddelen
- Wachtwoordpolicy;
- Toepassing van cryptografische hulpmiddelen;
- Classificatierichtlijnen;
- Policy voor het afsluiten van servers en werkstations;

5.4 Controle, naleving en sancties

Bij Onderwijsgroep Tilburg initieert de Coördinator informatiebeveiliging i.o.m de functionaris gegevensbescherming in samenwerking met de interne auditor de controle op de uitvoering van de informatiebeveiligings en privacy jaarplannen. De externe controle wordt uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning Control en verantwoordingscyclus.
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 de Onderwijsgroep Tilburg.

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.

De functionaris gegevensbescherming heeft een belangrijke toezichthoudende rol op de verwerking van persoonsgegevens. De functionaris gegevensbescherming controleert de naleving op het gebied van relevante privacywetgeving. Daarnaast adviseert de functionaris gegevensbescherming over de uitvoering van de privacywetgeving, helpt hij bij het opstellen van privacybeleid en is hij aanspreekpunt voor betrokkenen. De functionaris gegevensbescherming wordt ingesteld door het College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

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 de Onderwijsgroep Tilburg 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 Coördinator Informatiebeveiliging en Privacy; uiteindelijk is ook hiervoor het College van Bestuur eindverantwoordelijk.

Organisatie van de informatiebeveiliging en privacy rollen (functies)
Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij de Onderwijsgroep Tilburg 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 de Onderwijsgroep Tilburg en stelt het beleid en de basis maatregelen op het gebied van informatiebeveiliging en privacy vast. De inhoudelijke verantwoordelijkheid voor informatiebeveiliging is gemandateerd aan de Coördinator informatiebeveiliging. De inhoudelijke verantwoordelijkheid voor de privacy is gemandateerd aan de functionaris gegevensbescherming. Deze hebben 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 de Onderwijsgroep Tilburg**.**

Coördinator informatiebeveiliging
De Coördinator informatiebeveiliging is een rol op tactisch niveau. Hij adviseert samen met de directeur BMO en Informatiemanager aan het College van Bestuur. De Coördinator informatiebeveiliging bewaakt de uniformiteit van informatiebeveiligingsmaatregelen binnen de instelling.

Functionaris gegevensbescherming
De functionaris gegevensbescherming houdt binnen Onderwijsgroep Tilburg toezicht op de toepassing en naleving van de relevante privacywetgeving, zoals de Algemene verordening gegevensbescherming. De wettelijke taken en bevoegdheden van de functionaris gegevensbescherming geven de functionaris gegevensbescherming een onafhankelijke positie in de organisatie.

Coördinator Functioneel beheerder
De coördinator functioneel beheer coördineert het functioneel beheer van onderwijs- of bedrijfsapplicatie en is vormgegeven op het stafniveau. Deze vervult een rol bij de vertaling van de tactische naar operationele plannen. Dit doet hij samen met de Coördinator informatiebeveiliging (vanwege de uniformiteit) en met de eigenaren van de applicaties en technische platforms.

Proceseigenaar
Een proceseigenaar is iemand die verantwoordelijk is voor een van de primaire of ondersteunende processen, zoals inkoop, HRM en onderwijs. Deze dienen te voldoen aan de informatiebeveiligingskaders die door OGT zijn vastgesteld.

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.

Eigenaar van een technisch platform
De eigenaar van een technisch platform is er verantwoordelijk voor dat de applicatie een goede ondersteuning biedt aan het proces waarvoor deze verantwoordelijk is. Dit betekent dat de platformeigenaar ervoor 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 basismaatregelen.

Informatiearchitect
De informatiearchitect adviseert over specifieke informatiebeveiligingsmaatregelen in projecten (hogere systemen) en bewaakt de consistentie van de maatregelen (dubbelrol voor informatiemanager).

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

- Ervoor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid.
- Toe te zien op de naleving van het beveiliging- en privacy beleid door zijn medewerkers.
- Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen.
- Als aanspreekpunt beschikbaar te zijn voor de 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 informatiebeveiliging- en privacybeleid en tenminste aan de basis maatregelen. De leidinggevende kan hierin ondersteund worden door de Coördinator informatiebeveiliging.

IRT-coördinator
De IRT-coördinator bij Onderwijsgroep Tilburg wordt benoemd door de directeur BMO op instellingsniveau en opereert in diens opdracht. Hij is bevoegd het isoleren van computersystemen of netwerksegmenten te gelasten.

5.6 Overleg

Om de samenhang in de organisatie van de informatiebeveiligingsfunctie en privacy 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 Onderwijsgroep Tilburg 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 SPIM overleg (tactisch/strategisch).

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 centraal (AP) georganiseerd.

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

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 Onderwijsgroep Tilburg is er daarom een meldpunt ingericht en is bekend gemaakt hoe dat is te benaderen.
Elke organisatorische eenheid is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging dan wel privacy. De lijnmanager dient de incidenten en inbreuken direct te melden aan het ICT meldpunt van Onderwijsgroep Tilburg (Servicedesk/Topdesk of direct contact op te nemen met coördinator informatiebeveiliging of functionaris gegevensbescherming).
Gezien de meldplicht datalekken die per 1 januari 2016 is opgenomen in de WBP heeft de Onderwijsgroep Tilburg een beleid en een protocol datalekken ontwikkeld. Daarin is beschreven op welke wijze binnen 72 uur 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) is aangewezen om deze melding te doen. De privacytoezichthouder College Bescherming Persoonsgegevens maakt in ene richtsnoer in december 2015 bekend op welke manieren een datalek moet worden gemeld. De incidenten worden geregistreerd volgens de standaard indeling eSCIRT.net Incident Classificatie, waardoor een objectieve vergelijking met incidenten bij andere instellingen mogelijk wordt. De incidenten worden door de functionaris gegevensbescherming afgehandeld en dienen als input voor de incident-rapportages, waarover in het operationeel overleg wordt gesproken. Bij constatering van bepaalde trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne.

6.2 Informatiebeveiliging en Privacy incident response Team (IRT)

Het doel van het IRT bij Onderwijsgroep Tilburg is instelling brede preventie en curatieve zorg voor o.a. informatiebeveiliging en privacy incidenten. Het IRT houdt zich ook bezig met beveiligingsincidenten buiten Onderwijsgroep Tilburg als daar eigen medewerkers of studenten in enige rol bij betrokken zijn. In zulke gevallen wordt in principe gebruik gemaakt van de diensten van SURFcert, die wereldwijd in verbinding staat met andere emergency response teams.
De leden van het IRT zijn benoemd door de directeur BMO en opereren in diens opdracht. Het IRT is gerechtigd het isoleren van computersystemen of netwerksegmenten te gelasten.

Het IRT van Onderwijsgroep Tilburg heeft t.a.v. informatiebeveiliging en privacy 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 aan directeur BMO en het SPIM over de beveiligingsincidenten en het doen van voorstellen tot betere preventie van of curatie op incidenten.

Het IRT bij Onderwijsgroep Tilburg levert t.a.v. informatiebeveiliging en privacy calamiteiten de volgende diensten:

- Afhandelen van binnenkomende e-mails
- Afhandelen van binnenkomende telefonische meldingen
- Inrichten en operationeel houden van een meldpunt voor alle beveiligings- en privacy incidenten en het coördineren en bewaken van een adequate afhandeling daarvan

- De bereikbaarheid van de IRT (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.

Het IRT bij Onderwijsgroep Tilburg behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiligings- c.q. privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.
De dienstverlening van het IRT bij Onderwijsgroep Tilburg is gedocumenteerd en door het College van Bestuur bekrachtigd.

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.