

Informatiebeveiligings- en privacybeleid Zadkine

op basis van ISO27001/2 en wetgeving



Naam document:	Informatiebeveiligings- En Privacy Beleid Zadkine Versie 1.0.Docx
Datum:	19-4-2016

0 Verantwoording

0.1 Document

Document voldoet aan inrichting en vormgeving ISO 27002

0.2 Bronnen

- Masterclass Informatiebeveiligingsbeleid (Kennisnet / saMBO-ICT)
- ISO Informatiebeveiliging Code informatiebeveiliging
- Stichting Surf
- Normenkader ISO 27001 en 27002
- Wet en regelgeving
- SamboICT/Kennisnet
 - Ludo Cuijpers (Leeuwenborgh)
 - Leo Bakker (Kennisnet)
 - Casper Schutte(ROC Midden Nederland)
 - Paulo Moekotte (ROC van Twente)
 - Job Vos (Kennisnet)

0.3 Bewerking

Voor Zadkine door: Dienst Informatiemanagement
Wim Arendse, adviseur informatiemanagement
Marcel van Oorscot, informatiemanager

0.4 Audit

Conform beleidslijn OCW, Peer-review door instellingen zelf door gecertificeerde auditors.

0.5 Verspreiding

Functie	Naam	Versie	Datum
Adviseur Informatiemanagement	Michiel Musters	Concept 0.3	22-01-2016
Adviseur Informatiemanagement	Wim Arendse		
Informatiemanager	Ileen Smits		
Informatiemanager	Marcel van Oorscot		
Procesbegeleiding AO/IC	Franck van Erck	Concept 0.4	22-01-2016
Adviseur Informatiemanagement	Wim Arendse		
Informatiemanager	Marcel van Oorscot		
Hoofd ICT	Roel Varossieau		
Hoofd AO	Alwin van Es	Definitief 1.0	08-04-2016
Regiegroep Informatievoorziening	Henk Slagt	Definitief 1.0	19-04-2016
CvB en Directie Zadkine	Robbert Poort	Definitief 1.0	19-04-2016

0.6 Goedkeuring

Functie	Naam	Versie	Datum goedkeuring
Regiegroep Informatievoorziening	Henk Slagt	Definitief 1.0	08-04-2016
DT	Luc Verburgh	Definitief 1.0	19-04-2016



Inhoudsopgave

0	Verantwoording.....	2
1.	Inleiding	5
1.1	Toelichting informatiebeveiliging beleid	5
1.2	Toelichting privacy beleid	5
1.3	Vervlechting informatiebeveiliging en privacy	5
1.4	Doelstelling informatiebeveiliging en privacy beleid	6
1.5	Beschermen van persoonsgegevens	6
2.	Beleidsprincipes informatiebeveiliging en privacy	7
2.1	Beleidsuitgangspunten informatiebeveiliging en privacy	7
2.2	Beleidsprincipes informatiebeveiliging en privacy	8
3.	Classificatie	9
4.	Wet- en regelgeving	11
4.1	Wettelijke voorschriften	11
4.1.1	Wet Educatie Beroepsvorming	11
4.1.2	Wet Bescherming Persoonsgegevens	11
4.1.3	Archiefwet	11
4.1.4	Auteurswet	11
4.1.5	Telecommunicatiewet	11
4.1.6	Wet Computercriminaliteit.....	11
4.2	Overige richtlijnen en landelijke afspraken.....	11
5.	Governance informatiebeveiliging en privacy beleid	12
5.1	Afstemming met aanpalende beleidsterreinen.....	12
5.2	Inpassing in de Zadkine IBP governance	12
5.3	De financiering van informatiebeveiliging	13
5.4	Documenten informatiebeveiliging en privacy.....	13
5.4.1	Het informatiebeveiliging en privacy beleid	13
5.4.2	Baseline van maatregelen (basisniveau maatregelen).....	13
5.4.3	Jaarplan/verslag	13
5.4.4	Business Continuity Plan	13
5.4.5	Diensten niveau overeenkomsten (SLA's)	13
5.4.6	Contracten applicaties en educatieve software	14
5.4.7	Inhuur- en uitbestedingscontracten.....	14
5.4.8	Policies	14
5.5	Controle, naleving en sancties	14
5.6	Bewustwording en training	14
5.7	Organisatie van de informatiebeveiliging en privacy functie	15
5.8	Overleg	16
6.	Melding en afhandeling van incidenten	17
6.1	Registratie informatiebeveiliging en privacy incidenten	17
6.2	Informatiebeveiliging en Privacy Crisis Team (IPCT).....	17
7.	Tenslotte	18
7.1	Managementsamenvatting	18
7.2	Pragmatische aanpak.....	18
8.	Bijlages	19
8.1	Planning op hoofdlijn	19
8.2	Investering (out of the pocket).....	19
	Bijlage 1: Toelichting beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.....	20
	Voorbeeld classificatie model.....	21

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 leggen¹.

Informatiebeveiliging is een beleidsverantwoordelijkheid van het bestuur van Zadkine. 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 imagooverlies.

Zadkine heeft de ambitie om met het onderhavige beleidsdocument 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 relatieduidelijk 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 Zadkine waaronder in ieder geval alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan Zadkine persoonsgegevens verwerkt.

In het beleid ligt de nadruk op de geheel of gedeeltelijk geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van Zadkine 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 Zadkine 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 Zadkine heeft als doel om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

Beoogd wordt de persoonlijke levenssfeer van de betrokkene zoveel mogelijk te respecteren. 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 Zadkine

1.3 Vervlechting informatiebeveiliging en privacy

Bij Zadkine wordt informatiebeveiliging (processen) gekoppeld aan privacy (mensen). Het informatiebeveiliging en privacy beleid binnen Zadkine heeft betrekking op alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur / outsourcing), alsmede op alle organisatieonderdelen. Tevens

¹ Zie bijlage 1 voor toelichting.

vallen onder het informatiebeveiliging en privacy beleid alle devices van waaraf geautoriseerde toegang tot het instellingsnetwerk verkregen kan worden.

Bij het informatiebeveiliging en privacy beleid ligt de nadruk op die toepassingen die vallen onder de verantwoordelijkheid van Zadkine. Dit heeft betrekking op *gecontroleerde informatie*, die door de instelling zelf is gegenereerd en wordt beheerd.

1.4 Doelstelling informatiebeveiliging en privacy beleid

Het informatiebeveiliging en privacy beleid bij Zadkine 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 informatiebeveiliging en privacy beleid voor Zadkine 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/wordt compliant met de Nederlandse en Europese wetgeving

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

1.5 Beschermen van persoonsgegevens

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

Opslag en verwerking van persoonsgegevens (Privacy) is noodzakelijk 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 Zadkine, maar ook aan Zadkine zelf (bijvoorbeeld imagoschade). Zadkine 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 Zadkine.

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

2. Beleidsprincipes informatiebeveiliging en privacy

2.1 Beleidsuitgangspunten informatiebeveiliging en privacy

De beleidsuitgangspunten bij Zadkine zijn:

- Informatiebeveiliging 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.
- Toegang tot informatiesystemen wordt verleend op basis van relevante wet- en regelgeving, in het bijzonder conform de Wet Bescherming Persoonsgegevens (2001). Hierbij dient een goede balans te worden aangebracht tussen het belang van Zadkine om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens.
 - De toegangsbeveiliging dient de volgende aspecten te waarborgen (zie ook bijlage 1):
 - Beschikbaarheid
 - Integriteit
 - Vertrouwelijkheid
 - Betrouwbaarheid.
- Toegang tot informatiesystemen wordt verleend op basis van een aan een autorisatiemodel gekoppeld medewerkersprofiel. Dit profiel wordt per functie opgesteld. Het feit dat we een school zijn kenmerkt zich onder meer door een transparant, open karakter. De toegang tot informatiesystemen kent echter geen open karakter en is daarmee minder open voor interne gebruikers, studenten, gasten, externen.
- 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 en geïmplementeerd voor computer- en internet gebruik.

Om aan bovenstaand beleidsuitgangspunt te voldoen hanteert Zadkine de volgende 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 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.
- Bij alle registraties op vrijwillige basis zal aan de betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden

2.2 Beleidsprincipes informatiebeveiliging en privacy

Zadkine hanteert de volgende beleidsprincipes:

- 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 continue processen. 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. 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 de eigenaar, houdt en beheert Zadkine 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 de 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.



3. Classificatie

Bij Zadkine 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:

- a. beschikbaarheid
- b. integriteit
- c. vertrouwelijkheid

A. Beschikbaarheid

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

Classificatie	Classificatie gevolg
Beschikbaarheid: Laag	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.
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.
Beschikbaarheid: Hoog	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 4 uur brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.

B. Integriteit

Voor integriteit wordt de volgende classificatie indeling gehanteerd:

Classificatie	Classificatie gevolg	Toelichting
Integriteit: Laag	Het bedrijfsproces staat enkele integriteitsfouten toe.	Dit is het basisniveau. Wanneer de data onjuist, onvolledig en niet op tijd is, dan gaat het proces gewoon door en zal de kwaliteit van het proces op gelijke hoogte blijven
Integriteit: Midden	Het bedrijfsproces staat zeer weinig integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk.	Wanneer de data onjuist, onvolledig en niet op tijd zijn, 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 studenten of medewerkers zal geen schade ontstaan. Er zijn geen gerechtelijke of financiële consequenties voor Zadkine.
Integriteit: Hoog	Het bedrijfsproces staat geen integriteitsfouten toe.	De data zijn zodanig vervuild of zodanig cruciaal dat dit ernstige gevolgen voor het proces heeft. Er kunnen fouten gemaakt zijn, die grote schade veroorzaakt hebben bij Zadkine. Het proces moet stilgelegd worden om verdere schade te beperken. Schade of foutieve conclusies kunnen plaatsvinden die financiële, gerechtelijke of andere consequenties kunnen voor Zadkine.

C. Vertrouwelijk

Vertrouwelijkheid is als volgt geclassificeerd:

Classificatie	Classificatie gevolg	Toelichting
Vertrouwelijkheid: Laag	Informatie die toegankelijk mag of moet zijn voor alle of grote groepen medewerkers of studenten. Vertrouwelijkheid is gering.	Iedereen mag bijvoorbeeld de gegevens inzien van de website van Zadkine. Een geselecteerde groep mag deze gegevens wijzigen

Vertrouwelijkheid: Midden	Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie is vertrouwelijk.	Alleen een (grote of kleine) groep medewerkers of studenten van Zadkine mag deze gegevens inzien; toegang kan zowel binnen als buiten de instelling (remote) worden verleend, bijvoorbeeld lesroosters of Elo. Een geselecteerde groep mag deze gegevens wijzigen
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.	Bv. Zorgdossier van studenten, van bedrijfsarts.

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.



4. Wet- en regelgeving

4.1 Wettelijke voorschriften

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

4.1.1 Wet Educatie Beroepsvorming

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

4.1.2 Wet Bescherming Persoonsgegevens

Zadkine heeft de wettelijke vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) geïmplementeerd via het informatiebeveiligingsbeleid. Naleving van de beveiligingsmaatregelen leidt deels tot voldoen aan de wet. Voor aanvullende maatregelen is een additioneel Privacy beleidsplan opgesteld.

4.1.3 Archiefwet

Zadkine 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

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

4.1.5 Telecommunicatiewet

Zolang het netwerk van Zadkine niet openbaar is, is de Telecommunicatiewet niet van toepassing². Instellingen die wel (ten dele) een openbaar netwerk aanbieden moeten aan de Telecommunicatiewet voldoen.

4.1.6 Wet Computercriminaliteit

De Wet Computercriminaliteit richt zich op 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 Zadkine moet leiden tot een niveau van beveiliging dat als voldoende mag worden gezien in het kader van de Wet Computercriminaliteit.

4.2 Overige richtlijnen en landelijke afspraken

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

- DUO afspraken Bron e.d.;
- Aansluitvoorwaarden SURFnet.

² Let op! Bij het faciliteren van gastaccounts wordt het netwerk in principe wel openbaar!

5. Governance informatiebeveiliging en privacy beleid

Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term governance. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de instelling, zoals de eigenaren, werknemers, 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 Zadkine op strategisch niveau zowel aandacht geschonken wordt aan informatiebeveiliging 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 in de Zadkine IBP governance

In deze paragraaf wordt beschreven hoe IBP-governance in Zadkine 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 Informatiebeveiliging en Privacy (afgekort als manager IBP) is een rol op strategisch en tactisch niveau. Hij adviseert samen met de Informatiemanager aan het DT College van Bestuur. De manager IBP bewaakt de uniformiteit binnen de instelling.

Op operationeel niveau voert de manager IBP overleg met de functionele (functioneel beheer Financien en functionele beheerders van bijvoorbeeld educatieve applicaties) en technische beheerders (waaronder ook DBA). 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 - Directeuren Onderwijs - Hoofd HR - Hoofd ICT	- CvB stelt vast - DT adviseert - Regiegroep Informatievoorziening 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 - Functioneel 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 Beheerders - ICT	Operationeel IBP overleg	- SLA's (security paragraaf) - Incident registratie, incl. evaluatie

5.3 De financiering van informatiebeveiliging

De financiering van informatiebeveiliging en privacy wordt bij Zadkine als volgt geregeld.

- Algemene zaken, zoals het opstellen van een informatiebeveiliging en privacy plan voor de gehele instelling of een externe audit, wordt bij Informatiemanagement (IM) gebudgetteerd. 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 communicatie, awareness en training: er kunnen instelling brede bewustwordingscampagnes zijn (centraal opgenomen in het IM budget) en lokale voorlichting en training voor specifieke toepassingen of doelgroepen (decentraal gebudgetteerd).

5.4 Documenten informatiebeveiliging en privacy

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

5.4.1 Het informatiebeveiliging en privacy beleid

Het informatiebeveiliging en privacy beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen de instelling. In het informatiebeveiliging 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 informatiebeveiliging en privacy beleid wordt opgesteld door de manager IBP en vastgesteld door het College van Bestuur.

5.4.2 Baseline van maatregelen (basisniveau maatregelen)

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

5.4.3 Jaarplan/verslag

Elk jaar levert de manager IBP een jaarverslag en een jaarplan voor het volgende jaar in bij de Regiegroep Integratie Informatievoorziening. 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.

5.4.4 Business Continuity Plan

Business Continuity Management (BCM) is de benaming van het proces dat potentiële bedreigingen voor een organisatie identificeert en bepaalt wat de impact op de "operatie" van de organisatie is als deze bedreigingen daadwerkelijk manifest worden. Het product van BCM bestaat uit een samenhangend stelsel van maatregelen, die zowel preventief, detectief, repressief als correctief werkzaam zijn. Het Business Continuity Plan wordt opgesteld door de Informatiemanager, in samenspraak met de proceseigenaren, Hoofd Facilitaire dienst, Hoofd IT, Hoofd AO, Hoofd FP&C.

5.4.5 Diensten niveau overeenkomsten (SLA's)

Een service level agreement is een overeenkomst tussen een leverancier en een afnemer met afspraken en randvoorwaarden over geleverde diensten. In deze contracten zit standaard een informatiebeveiligingsparagraaf, waarin de verantwoordelijkheden van de leverancier zijn opgenomen. Alle SLA's worden om die reden voorgelegd aan de manager IBP.

5.4.6 Contracten applicaties en educatieve software

Met alle leveranciers van onderwijs- en bedrijfsapplicaties en educatieve software worden bewerkers-overeenkomsten afgesloten. Dit geldt ook voor overheids- en ander instellingen indien er data van studenten of medewerkers wordt verstrekt, al dan niet op wettelijke basis. Alle contracten met voornoemde leveranciers worden om die reden voorgelegd aan de manager IBP en Functionaris Gegevensbescherming.

5.4.7 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. Deze bepaling dient in het inhuurcontract te worden opgenomen. Hetzelfde is van belang bij uitbestedingen.

5.4.8 Policies³

Er zijn gedragscodes en richtlijnen voor medewerkers, studenten en derden opgesteld, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging.

Zoals:

- Acceptable use policy, voor het veilig gebruik van ICT-voorzieningen;
- Wachtwoordpolicy;
- 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.

5.5 Controle, naleving en sancties

Bij Zadkine 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). Zadkine is voorstander van deelname aan de branche audit voor het MBO. De bevindingen van de interne en externe audits zijn input voor de nieuwe jaarplannen van Zadkine.

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. Mocht de naleving ernstig tekort schieten, dan kan Zadkine de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden. Het toewijzen van de rol FG aan een geschikte functionaris is daarom essentieel.

5.6 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 Zadkine 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, studenten 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 bewustzijn op het gebied van informatiebeveiliging en privacy is een verantwoordelijkheid van de manager IBP die rapporteert aan het College van Bestuur als eindverantwoordelijke.

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

5.7 Organisatie van de informatiebeveiliging en privacy functie

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Zadkine 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 Zadkine en stelt, in overleg met het DT, 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 manager IBP. 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 Zadkine.

Manager IBP

De manager IBP is een rol op strategische (en tactisch) niveau binnen de taken van een adviseur Informatiemanagement.

Functioneel beheerder

De rol van functioneel beheerder onderwijs- of bedrijfsapplicatie is de schakel tussen beleid en uitvoering naar de applicaties en data. Dit doen ze samen met de manager IBP 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

De functionaris voor de gegevensbescherming (FG) houdt binnen Zadkine 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.

CERT-coördinator

CERT staat voor Computer Emergency Response Team. Dit is een gespecialiseerd team van ICT-professionals, dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken. Het doel is om schade te reduceren en snel herstel van de dienstverlening te bevorderen. De CERT-coördinator bij Zadkine wordt benoemd door het hoofd ICT op instellingsniveau en opereert in diens opdracht. Hij is bevoegd het isoleren van computersystemen of netwerksegmenten te gelasten.

5.8 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 Zadkine gestructureerd overleg gevoerd over het onderwerp informatiebeveiliging en privacy op vele 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 de regiegroep Informatievoorziening.

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 applicatie portaal of dienst georganiseerd en rapporteert aan de Regiegroep Integrale Informatievoorziening.

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 commercieel.

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 Zadkine 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 of privacy. De lijnmanager dient de incidenten en inbreuken direct te melden aan de Servicedesk van Zadkine.

De incidenten worden geregistreerd in TopDesk met een classificatie volgens een saMBO-ICT standaard (zie hoofdstuk 3), waardoor een objectieve vergelijking met incidenten bij andere instellingen mogelijk wordt. De incidenten worden 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 Crisis Team (IPCT)

Het doel van het Informatiebeveiliging en Privacy Crisis Team (IPCT) bij Zadkine is instelling brede preventie en curatieve zorg voor informatiebeveiliging en privacy incidenten. Het IPCT houdt zich ook bezig met beveiligingsincidenten buiten Zadkine als daar eigen medewerkers of studenten 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 Bestuur en opereren in diens opdracht. De CERT-coördinator maakt in ieder geval deel uit van het IPCT.

Het IPCT is gerechtigd het isoleren van computersystemen of netwerksegmenten te gelasten.

Het IPCT van Zadkine heeft de volgende opdracht:

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

Het IPCT bij Zadkine 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 beveiligings en privacy aspecten
- Periodiek opstellen van managementrapportages;
- Optie: Onderhoudt contacten met SURFcert.

Het IPCT bij Zadkine 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 Zadkine is gedocumenteerd en door het College van Bestuur bekrachtigd.

De rol van IPCT coördinator wordt belegd bij de manager IBP.

7. Tenslotte

7.1 Managementsamenvatting

Het Informatiebeveiliging en Privacy beleid geeft antwoord op de vraag: waarom is informatiebeveiliging en privacy belangrijk voor Zadkine?

Elke organisatie is zelf verantwoordelijk voor de eigen Informatiebeveiliging en Privacy. Deze verplichting is niet uit te besteden aan een derde partij. Zadkine kent en onderkent deze verantwoordelijkheid ten opzichte van studenten, medewerkers en de maatschappij ten aanzien van waarborging van privacy, continuïteit en veiligheid in onze informatiesystemen.

Daarnaast kennen we vanuit wet- en regelgeving verplichtingen ten aanzien van het beveiligen van informatie en kan Zadkine daarvoor ook aansprakelijk worden gesteld.

Vanuit die optiek dienen CvB, DT en lijnmanagement van de organisatie hun eigen verantwoordelijkheid te nemen. Was het eerst voldoende wanneer de wetten en regels precies werden nageleefd, tegenwoordig luidt de vraag: heeft de organisatie al het mogelijke gedaan om een bepaald incident te voorkomen of de daaruit voortvloeiende schade zoveel mogelijk te beperken?

Dit is een heel andere insteek en vergt een andere manier van denken. Geredeneerd vanuit deze nieuwe verantwoordelijkheid dient Zadkine zich adequaat te beraden op de vraag hoe ze informatiebeveiliging en privacy vorm wil geven. Vanuit wet- en regelgeving is één ding. Een geborgde bedrijfsvoering is een andere. Daarnaast moet ook de nodige aandacht besteed worden aan de in- en externe contracten en sla's.

7.2 Pragmatische aanpak

Het Informatiebeveiliging en Privacy beleid is gericht op de basisbeveiliging en continuïteit die vanuit wetgeving en eigen verantwoordelijkheid naar medewerkers en studenten vereist zijn.

Zadkine kiest voor een pragmatische invulling ('lean and mean') van de informatiebeveiliging op basis van de Code voor Informatiebeveiliging. Dit stelt ons in staat om beveiliging op maat te voeren door bewust te kiezen welke maatregelen wel en welke niet worden doorgevoerd.

Privacy is nauwverwant met informatiebeveiliging en wordt samen met informatiebeveiliging opgepakt. Omdat privacy een veel strakkere regelgeving kent vanuit de Wet bescherming persoonsgegevens (Wpb), die in Europeesverband dit jaar verder wordt aangescherpt, wordt de (nieuwe) Wpb ook als uitgangspunt genomen.

Waar mogelijk worden meerdere rollen belegd bij één persoon of nieuwe rollen bij bestaande functies ondergebracht en worden overleggen in de bestaande overlegstructuren geïntegreerd.

8. Bijlages

8.1 Planning op hoofdlijn

Detail planning wordt opgenomen in Plan van Aanpak

Activiteit	2016											
	jan	feb	mrt	apr	mei	juni	juli	aug	sept	okt	nov	dec
Vaststellen Informatiebeleidsplan												
Opleiden manager IBP (2)												
Privacy training (2)												
Plan van Aanpak												
Vooronderzoek/bepalen complexiteit												
Vaststellen scope												
Awareness campagne, take off												
Implementatie												
Audit ISO 27002												
Audit-certificaat/beoordeling												
Legenda	in uitvoering	gerealiseerd	gepland									

8.2 Investerings (out of the pocket)

Uitwerking in detail in Plan van Aanpak

Product	Out of the Pocket	Inzet intern	Inzet extern
Opleidingen	3k (IM 2015)	22 dagen	
Externe consulting	10k	1 dag	10 dagen
Nul meeting	12k	15 dagen	8 dagen
Awareness campagne	10k	10 dagen	?
Implementatie	10k	40 dagen	
Audit PWC(?)	Ntb*	?*	?*
Verkrijgen certificaat	8k	2 dagen	1 dag
Totalen	53k*	90 dagen*	19 dagen*

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

	Definitie	Classificatie inde- ling	Classificatie gevolg	Beheersmaatregel	Audit
Beschikbaar- heid	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.	Beschikbaarheid Laag	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	• Beschikbaarheid netwerk standaard. • Standaard back up en restore test	Procescontrole plus controle beschikbaarheid test.
		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.	• Beschikbaarheid netwerk standaard. • Regelmatig back up en restore test	Procescontrole plus controle beschikbaarheid test.
		Beschikbaarheid Hoog	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 4 uur brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	• Standaard netwerk plus reserve netwerk • Regelmatig back up en restore test	Procescontrole plus controle beschikbaarheid test.
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.	Integriteit Laag	Het bedrijfsproces staat enkele integriteitsfouten toe.	• Application controls	Procescontrole
		Integriteit Midden	Het bedrijfsproces staat zeer weinig integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk.	• Application controls • Manual controls	Procescontrole
		Integriteit Hoog	Het bedrijfsproces staat geen integriteitsfouten toe.	• Application controls • Manual controls • 4 ogen principe	Procescontrole plus verbandscontrole
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.	Vertrouwelijkheid Laag	Informatie die toegankelijk mag of moet zijn voor alle of grote groepen medewerkers of studenten. Vertrouwelijkheid is gering.	• Generieke toegangsbeveiliging	Procescontrole

	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.	Vertrouwelijkheid Midden	Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie is vertrouwelijk.	• Autorisatiematrix	Procescontrole plus verbandscontrole
		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.	• Autorisatiematrix • Soft token • Encryptie	Procescontrole plus verbandscontrole
Privacy	Algemeen beleidsuitgangspunt is dat Persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Hierbij dient een goede balans te worden aangebracht tussen het belang van <de instelling> om Persoonsgegevens te verwerken en het belang van Betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn Persoonsgegevens.	Vertrouwelijkheid Laag, Midden en Hoog 1	Er wordt voldaan aan de privacy wetgeving, uitgezonderd bijzondere persoonsgegevens.	• Beleid • Awareness	Procescontrole
		Vertrouwelijkheid Hoog 2	Er wordt voldaan aan de privacy wetgeving, inclusief bijzondere persoonsgegevens.	• Beleid • Awareness • Portfolio opslag, dus niet digitaal	Procescontrole plus verbandscontrole

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.