Normenkader informatiebeveiliging mbo

IBPDOC2A

GEBRUIKERSGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Verantwoording

Bron:

Normenkader Informatiebeveiliging HO 2015
Gebaseerd op ISO 27002:2013
Stichting SURF
April 2015

Met dank aan:

Maturity Werkgroep SURFibo:

- Hans Alfons (Vrije Universiteit)
- Ludo Cuijpers (saMBO-ICT en Kennisnet)
- Bart van den Heuvel (Universiteit Maastricht)
- Alf Moens (SURF)
- Menno Nonhebel (KNAW)
- Anita Polderdijk-Rijntjes (Christelijke Hogeschool Windesheim)
- Rene Ritzen (Universiteit Utrecht)
- Ron Veldhoen (Universiteit Twente)

SURFibo

Het SURF Informatie Beveiligers Overleg is een community of practice binnen SURF samenwerkingsorganisatie met als doelen het actief stimuleren van en richting geven aan informatiebeveiliging binnen het hoger onderwijs en onderzoek (universiteiten, hogescholen, wetenschappelijk onderzoek en universitair medische centra). Dat wordt bereikt door het bevorderen van de samenwerking tussen informatiebeveiligers/kwartiermaker IB en het leveren van praktisch bruikbare adviezen.
Voor meer informatie zie www.surfibo.nl

Bewerkt door:

Kennisnet / saMBO-ICT

Auteurs

Hans Hoogduijn (ID College)
Victor Hunnik (Grafisch Lyceum Rotterdam)
Ludo Cuijpers (Leeuwenborgh)
April 2015

Sommige rechten voorbehouden

Inhoudsopgave

1. Inleiding

Het Normenkader informatiebeveiliging mbo is een onderdeel van het Framework ibp in het mbo. Het normenkader geeft eenduidig weer welke maatregelen een instelling voor middelbaar beroepsonderwijs moet nemen op het gebied van informatiebeveiliging en voor de bescherming van persoonsgegevens. In dit document wordt het Normenkader informatiebeveiliging mbo toegelicht en worden de keuzes die gemaakt zijn bij de samenstelling van dit normenkader onderbouwd.

1.1 Gebruik van het normenkader

Het Normenkader informatiebeveiliging mbo wordt in de mbo-sector gebruikt als referentie voor informatiebeveiliging. Het wordt voor dit zelfde doel ook gebruikt in de ho sector**.** Op basis van dit normenkader kan een instelling bepalen of zij voldoet aan de eisen die gesteld worden. Bij het Normenkader informatiebeveiliging mbo hoort een toetsingskader[1]. In dit toetsingskader staat in detail beschreven wat een instelling geregeld moet hebben om aan de normen te voldoen. Dat toetsingskader is een separaat document, is opgesteld door interne auditors van de instellingen en afgestemd met informatiebeveiligers van de instellingen en externe auditpartijen, onder meer met de auditors van de grootste accountsbureaus.
Het Normenkader informatiebeveiliging mbo is de basis voor audits, self-assessments en peer-reviews in het kader van MBOaudit.

1.2 Historie en beheer

Het Normenkader informatiebeveiliging mbo vervangt eerdere versies van het normenkader informatiebeveiliging, te weten de versie 1.0. Deze 2015 versie wordt geëvalueerd en zo nodig bijgesteld voor publicatie na de zomer van 2016. In het najaar van 2016 zal een revisie groep onder leiding van SURF aan een geheel nieuwe versie gaan werken.

De basis van het normenkader is in 2011 gelegd door het hoger onderwijs, was beperkt van opzet en omvatte die maatregelen die destijds voor het Hoger Onderwijs van essentieel belang waren. Dit normenkader was mede gebaseerd op de normselectie die ziekenhuizen bij hun toetsing voor de NEN7510 in 2010 gebruikt hebben. In 2013 is dit normenkader uitgebreid met de normen uit de Richtsnoer Beveiliging Persoonsgegevens van het College Bescherming Persoonsgegevens (CBP). Het Normenkader hoger onderwijs is op enkele punten verder uitgebreid en aangepast op de nieuwe versie van de onderliggende ISO 27002 standaard.

1.3 Verantwoording

Aan de totstandkoming van deze versie van het Normenkader IBHO15 is een bijdrage geleverd door de leden van de maturity werkgroep van SURFibo: Anita Polderdijk-Rijntjes, Bart van den Heuvel, Hans Alfons, Ludo Cuijpers, Menno Nonhebel, René Ritzen en Ron Velthoen. Dit document is besproken en goedgekeurd in de vergadering van de taskforce informatiebeveiliging en privacy mbo onderwijs op 28 mei 2015.

[1] Toetsingskader IB: clusters 1 t/m 6 (IBPDOC3)

2. Samenstelling Normenkader informatie-beveiliging mbo

Het Normenkader informatiebeveiliging mbo bestaat uit een selectie van de maatregelen uit ISO 27002 en omvat die maatregelen die van belang zijn voor het **mbo onderwijs**. De maatregelen zijn in zes logische clusters opgedeeld. De selectie van maatregelen is gebaseerd op praktijkervaringen in de verschillende sectoren en op risico evaluaties.

2.1 ISO 27000 familie

ISO27002 is de dé facto internationale standaard op het gebied van informatiebeveiliging. In 2013 is een herziene versie van deze standaard gepubliceerd. Het Normenkader informatiebeveiliging mbo is gebaseerd op ISO27002:2013. Naast de ISO 27002 wordt ook de ISO27001 veel gebruikt, deze beschrijft het procescontrole systeem (information security management system, ISMS) voor informatiebeveiliging. Instellingen worden aangeraden conform ISO 27001 hun informatiebeveiligingsprocessen in te richten. Eind 2014 is ook de ISO27018 standaard verschenen. Dit is een verdere detaillering van de ISO 27002 norm, specifiek voor PII (Personally Identifiable Information), privacy gevoelige informatie. In het Normenkader informatiebeveiliging mbo zijn alle privacy aspecten opgenomen die genoemd zijn in de Richtsnoer Beveiliging Persoonsgegevens van het CBP (CBP, 2013), hiermee is ook de basis van ISO 27018 afgedekt.

2.2 Clustering

De maatregelen in het Normenkader informatiebeveiliging mbo zijn gegroepeerd in 6 clusters. Deze clusters groeperen maatregelen die logischerwijs met elkaar samenhangen. Hiermee kan inzichtelijk gemaakt worden op welk onderdeel (beleid, personeel, fysieke beveiliging, continuïteit ed.) een instelling sterk of zwak is en kunnen inspanningen voor verbetering en controle beter en in samenhang gestuurd worden.

		Clusterindeling Hoger Onderwijs						
Hoofdstukken ISO-27002	ISO-27002	**1**: Beleid	**2**: personeel	**3**: Ruimten	**4**: Continuïteit	**5**: Toegang	**6**: Controle	Niet gebruikt
5. Informatiebeveiligingsbeleid	**2**	2						
6. Organiseren van informatiebeveiliging	**7**	4		0				3
7. Veilig personeel	**6**		3					3
8. Beheer van bedrijfsmiddelen	**10**	2		1				7
9. Toegangsbeveiliging	**14**		1			9	1	3
10. Cryptografie	**2**	1				1		
11. Fysieke beveiliging en beveiliging van de omgeving	**15**	1	1	12				1
12. Beveiliging bedrijfsvoering	**14**			1	7	1	2	3
13. Communicatiebeveiliging	**7**	2	1			4		
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	**13**	1			1	1	3	7
15. Leveranciersrelaties	**5**	2			1		1	1
16. Beheer van informatiebeveiligingsincidenten	**7**	2	1		2		1	1
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	**4**				2			2
18. Naleving	**8**	2					2	4
	114	**19**	**7**	**14**	**13**	**16**	**10**	**35**
Clustertotaal inclusief splitsing (85)		21	7	15	15	17	10	

tabel 1: samenhang ISO-27002 normenkader en Normenkader IBHO15

Een uitgewerkte verantwoording van de gebruikte statements uit het ISO-27002 normenkader en de "vertaling" naar het Normenkader informatiebeveiliging mbo is beschreven in bijlage 1.

2.3 Motivatie keuze maatregelen

Het Normenkader informatiebeveiliging mbo bevat een selectie van de maatregelen uit de ISO27002. Deze selectie is in 2011 klein begonnen met een kernpakket en in de afgelopen jaren gegroeid, op basis van een analyse van wet- en regelgeving, met name de privacy wetgeving, en op een risico afweging en evaluatie.

Risico Afweging
De samenstelling van het Normenkader informatiebeveiliging mbo is gebaseerd op een toets van de wettelijke verplichtingen in combinatie met een risico afweging. De belangrijkste relevante wettelijke verplichting is de Wet Bescherming Persoonsgegevens (Wbp), in het Normenkader informatiebeveiliging mbo zijn de beveiligingsrichtlijnen uit de Richtsnoer Beveiliging Persoonsgegevens van het College bescherming Persoonsgegevens (CBP) opgenomen. De risico afweging is gebaseerd op de belangrijkste bevindingen uit het Cyberdreigingsbeeld Hoger Onderwijs 2014.

Cyberdreigingsbeeld[2]
In 2014 heeft SURF, in samenwerking met het OCW-project Integrale Veiligheid, een onderzoek laten uitvoeren om te komen tot het Cyberdreigingsbeeld Hoger Onderwijs 2014. Dit rapport beschrijft de grootste dreigingen voor de sectoren hoger onderwijs en wetenschappelijk onderzoek op het gebied van informatieveiligheid. Deze dreigingen zijn uitgewerkt voor de hoofdprocessen Onderwijs, Onderzoek en Bedrijfsvoering. Op basis van de uitkomsten en aanbeveling in dit rapport is het normenkader informatiebeveiliging geanalyseerd op compleetheid. Hierbij is zowel gekeken welke maatregelen ín het normenkader een bijdrage leveren aan het beheersbaar maken of voorkomen van de belangrijkste 7 dreigingen (zie tabel 1), als naar welke maatregelen buiten het normenkader ten onrechte niet opgenomen zijn en toegevoegd moeten worden. Als resultaat van deze analyse is het normenkader op enkele punten uitgebreid.

Dreigingen
Verkrijging en openbaarmaking van data
Identiteitsfraude
Manipulatie van data
Spionage
Verstoring ICT
Overname en misbruik van ICT
Bewust beschadigen van imago

Tabel 1 De belangrijkste dreigingen voor het hoger onderwijs en het wetenschappelijk onderzoek

Verder ontwikkeling normenkader
Het Normenkader informatiebeveiliging mbo zal eind 2015 geëvalueerd en eind 2016 herzien worden. De evaluatie eind 2015 is bedoeld om kleine omissies aan te passen, met name tekstueel en in het toetsingskader. Eind 2016 wordt het normenkader structureel herzien. Dan wordt als uitgangspunt de hele ISO27002 genomen en zullen slechts enkele maatregelen buiten de scope geplaats worden op basis van een hernieuwde risico analyse en alleen met duidelijke motivatie.

[2] Voor de mbo sector zijn deze dreigingen herkenbaar (wellicht behalve spionage) en dus ook meegenomen in het Normenkader informatiebeveiliging mbo..

2.4 Volwassenheidsniveau

Het Normenkader informatiebeveiliging mbo wordt gebruikt om de volwassenheid van informatiebeveiliging te meten bij de mbo instellingen. Hiervoor wordt een 5-punts schaal gehanteerd gebaseerd op het Capability Maturity Model (CMM). Het CMM model is gebaseerd op procesvolwassenheid, de 5 niveaus staan in tabel 2 weergegeven.

CMM niveau	Omschrijving
1	Initieel, ad hoc: De processen zijn ad hoc georganiseerd, erg afhankelijk van individuele personen
2	Herhaalbaar, maar intuïtief: Er wordt op een vaste manier gewerkt
3	Gedefinieerd proces: De processen zijn gedocumenteerd en bekend bij betrokkenen
4	Beheerd en meetbaar: De processen worden beheerd, zitten in een verbetercyclus en zijn meetbaar. (PDCA)
5	Geoptimaliseerd: Er wordt als vanzelfsprekend verbeterd en volgens best practices gewerkt.

Tabel 2 De CMM niveaus

2.5 Toetsingskader

In aanvulling op het Normenkader informatiebeveiliging mbo is een toetsingskader beschikbaar. In dit toetsingskader is voor iedere maatregel in het normenkader beschreven wat de vereisten zijn om aan een volgende volwassenheidsniveau te voldoen. Het toetsingskader is opgesteld in nauwe samenwerking met de interne auditors van de universiteiten en afgestemd met externe auditors. Het is vervolgens voor de mbo sector bewerkt door medewerkers van saMBO-ICT en Kennisnet.

3. Het Normenkader

In de volgende paragrafen staat in tabelvorm het Normenkader informatiebeveiliging mbo beschreven. Per maatregel uit de norm staat het referentie nummer uit de ISO27002 genoemd, een korte omschrijving van de maatregel, een verklaring over de herkomst van de norm. Bij de start waren 36 statements in gebruik. Inmiddels is dit aantal gegroeid tot 85 statements.

Herkomst/ bron	Omschrijving
B (36 statements)	Basisnorm, vanaf de eerste versie opgenomen in normenkader, de minimale set.
P (31 statements)	Toegevoegd op basis van de Richtsnoer bescherming persoonsgegevens van het CBP
I (12 statements)	Toegevoegd wegens uitbreiding van de ISO27002:2013
D (4 statements)	Toegevoegd op basis van analyse van het Cyberdreigingsbeeld HO 2014.
B/I of P/I (2 statements)	Norm is enigszins aangepast in ISO 27002:2013

Tabel 3 Herkomst/Bron van maatregelen in Normenkader informatiebeveiliging mbo

3.1 Beleid en organisatie

Nr.	ISO27002	Statement	
1.1	**5.1.1.1**	**Beleidsregels voor informatiebeveiliging**: Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur.	**B-1**
1.2	**5.1.1.2**	**Beleidsregels voor informatiebeveiliging**: Het door het bestuur vastgestelde Informatiebeveiligingsbeleid wordt gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	**B-2**
1.3	**5.1.2**	**Beoordeling van het Informatiebeveiligingsbeleid**: Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	**B-3**
1.4	**6.1.1**	**Taken en verantwoordelijkheden informatiebeveiliging**: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen	**B-4**
1.5	**6.1.5**	**Informatiebeveiliging in projectbeheer**: Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	**I-1**
1.6	**6.2.1.1**	**Beleid voor mobiele apparatuur:** Er dient beleid te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	**I-2**
1.7	**8.2.1**	**Classificatie van informatie:** Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	**B-5**
1.8	**8.2.2**	**Informatie labelen:** Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	**P-1**
1.9	**10.1.1.1**	**Beleid inzake het gebruik van cryptografische beheersmaatregelen**: Ter bescherming van informatie behoort een beleid voor het gebruik van crypto grafische beheersmaatregelen te worden ontwikkeld.	**P-2**

Nr.	ISO27002	Statement	
1.10	10.1.1.2	**Beleid inzake het gebruik van cryptografische beheersmaatregelen:** Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van crypto grafische beheersmaatregelen wordt geïmplementeerd.	P-3
1.11	11.2.5	**Verwijdering van bedrijfsmiddelen:** Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	P-4
1.12	13.2.1	**Beleid en procedures voor informatietransport:** Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	B-6
1.13	13.2.2	**Overeenkomsten over informatietransport:** Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	B-7
1.14	14.1.1	**Analyse en specificatie van informatiebeveiligingseisen**: De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	B-8
1.15	15.1.2	**Opnemen van beveiligingsaspecten in leveranciersovereenkomsten**: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	P-5
1.16	15.1.3	**Toeleveringsketen van informatie- en communicatietechnologie:** Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	I-3
1.17	16.1.1	**Verantwoordelijkheden en procedures:** Er zijn leidinggevende en -procedures vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	B-9
1.18	16.1.2	**Rapportage van informatiebeveiligingsgebeurtenissen**: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	B-10
1.19	18.1.3	**Beschermen van registraties:** Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	I-4
1.20	18.1.4	**Privacy en bescherming van persoonsgegevens**: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	B-11
1.21	6.1.2	**Scheiding van taken:** Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	D-1

3.2 Personeel, studenten en gasten

Nr.	ISO27002	Statement	
2.1	7.1.2	**Arbeidsvoorwaarden**: De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	B-12
2.2	7.2.2	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging:** Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	B-13
2.3	9.2.6	**Toegangsrechten intrekken of aanpassen:** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	B-14
2.4	11.2.9	**'Clear desk'- en 'clear screen'-beleid**: Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten te worden ingesteld.	B-15
2.5	13.2.4	**Vertrouwelijkheids- of geheimhoudingsovereenkomst:** Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	P-6
2.6	16.1.3	**Rapportage van zwakke plekken in de informatiebeveiliging:** Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	P-7
2.7	7.1.1	**Screening**: Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.	D-2

3.3 Ruimtes en apparatuur

Nr.	ISO27002	Statement	
3.1	6.2.1.2	**Beleid voor mobiele apparatuur:** Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.	I-5
3.2	8.3.2	**Verwijderen van media:** Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	P-8
3.3	11.1.1	**Fysieke beveiligingszone:** Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	P-9
3.4	11.1.2	**Fysieke toegangsbeveiliging:** Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	B-16
3.5	11.1.3	**Kantoren, ruimten en faciliteiten beveiligen:** Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	P-10
3.6	11.1.4	**Beschermen tegen bedreigingen van buitenaf:** Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	P-11
3.7	11.1.5	**Werken in beveiligde gebieden:** Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	B-17
3.8	11.1.6	**Laad- en loslocatie:** Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.	P-12
3.9	11.2.1	**Plaatsing en bescherming van apparatuur:** Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	P-13
3.10	11.2.2	**Nutsvoorzieningen:** Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	P-14
3.11	11.2.3	**Beveiliging van bekabeling:** Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	P-15
3.12	11.2.4	**Onderhoud van apparatuur:** Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	B-18
3.13	11.2.6	**Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein:** Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	P-16
3.14	11.2.7	**Veilig verwijderen of hergebruiken van apparatuur:** Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	I-6
3.15	12.4.4	**Kloksynchronisatie:** De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	P-17

3.4 Continuïteit

Nr.	ISO27002	Statement	
4.1	12.1.2	**Wijzigingsbeheer:** Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	B-19
4.2	12.1.4	**Scheiding van ontwikkel-, test- en productieomgevingen** Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	D-3
4.3	12.2.1.1	**Beheersmaatregelen tegen malware:** Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd.	B-20
4.4	12.2.1.2	**Beheersmaatregelen tegen malware:** Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten ten aanzien van het gevaar van virussen en dergelijke.	B-21
4.5	12.3.1.1	**Back-up van informatie:** Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt.	B-22
4.6	12.3.1.2	**Back-up van informatie:** Gemaakte back ups worden regelmatig getest conform het back-up beleid.	B-23
4.7	12.5.1	**Software installeren op operationele systemen:** Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	D-4
4.8	12.6.1	**Beheer van technische kwetsbaarheden:** Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.	I-7
4.9	12.6.2	**Beperkingen voor het installeren van software:** Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	I-8
4.10	14.2.6	**Beveiligde ontwikkelomgeving:** Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	I-9
4.11	15.2.2	**Beheer van veranderingen in dienstverlening van leveranciers:** Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	P-18
4.12	16.1.4	**Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen:** Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiliging incidenten.	P-19
4.13	16.1.5	**Respons op informatiebeveiligingsincidenten:** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	B-24
4.14	17.1.2	**Informatiebeveiligingscontinuïteit implementeren:** De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	B-25
4.15	17.2.1	**Beschikbaarheid van informatie verwerkende faciliteiten:** Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	B-26

3.5 Vertrouwelijkheid en integriteit

Nr.	ISO27002	Statement	
5.1	9.1.1	**Beleid voor toegangsbeveiliging:** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	B-27
5.2	9.1.2	**Toegang tot netwerken en netwerkdiensten:** Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	I-10
5.3	9.2.1	**Registratie en afmelden van gebruikers:** Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	B-28
5.4	9.2.2	**Gebruikers toegang verlenen:** Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	I-11
5.5	9.2.3	**Beheren van speciale toegangsrechten:** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	B-29
5.6	9.2.4	**Beheer van geheime authenticatie-informatie van gebruikers:** Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	B-30
5.7	9.3.1	**Geheime authenticatie-informatie gebruiken:** Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie informatie houden aan de praktijk van de organisatie.	B-31
5.8	9.4.1	**Beperking toegang tot informatie:** Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	B-32
5.9	9.4.2	**Beveiligde inlogprocedures:** Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	B-33
5.10	10.1.2.1	**Sleutelbeheer:** Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld.	P-20
5.11	10.1.2.2	**Sleutelbeheer:** Er wordt gebruik gemaakt van tools om cryptografische sleutels tijdens hun gehele levenscyclus adequaat te beheren.	P-21
5.12	12.4.2	**Beschermen van informatie in logbestanden:** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	P-22
5.13	13.1.1	**Beheersmaatregelen voor netwerken:** Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	B/I
5.14	13.1.2	**Beveiliging van netwerkdiensten:** Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	I-12
5.15	13.1.3	**Scheiding in netwerken:** Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	B-34
5.16	13.2.3	**Elektronische berichten**: Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd	B-35
5.17	14.1.3	**Transacties van toepassingen beschermen:** Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	B-36

3.6 Controle en Logging

Nr.	ISO27002	Statement	
6.1	9.2.5	**Beoordeling van toegangsrechten van gebruikers:** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	P-23
6.2	12.4.1	**Gebeurtenissen registreren:** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	P-24
6.3	12.4.3	**Logbestanden van beheerders en operators:** Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	P-25
6.4	14.2.7	**Uitbestede softwareontwikkeling:** Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	P/I
6.5	14.2.8	**Testen van systeembeveiliging:** Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	P-26
6.6	14.2.9	**Systeemacceptatietests:** Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	P-27
6.7	15.2.1	**Monitoring en beoordeling van dienstverlening van leveranciers:** Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	P-28
6.8	16.1.7	**Verzamelen van bewijsmateriaal:** De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	P-29
6.9	18.2.2	**Naleving van beveiligingsbeleid en –normen:** Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	P-30
6.10	18.2.3	**Beoordeling van technische naleving:** Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	P-31

4. Ten slotte

4.1 Besluitvorming

Het Normenkader IBHO15 wordt behandeld in de stuurgroep Informatiebeveiliging en Privacy HO. Het is opgeleverd door de maturity werkgroep van SURFibo en goedgekeurd door de stuurgroep van SURFibo. Na behandeling in de stuurgroep Informatiebeveiliging en privacy HO wordt het normenkader voorgelegd aan CIO beraad, CvDUR en COMIT voor accordering. Het afgeleide MBO document (Normenkader informatiebeveiliging mbo) is goedgekeurd door de Taskforce Informatiebeveiliging.

4.2 Beheer van het normenkader informatiebeveiliging

Het beheer van het normenkader informatiebeveiliging, en specifiek deze laatste versie Normenkader informatiebeveiliging mbo, is belegd bij de maturity werkgroep van SURFibo. De stuurgroep van SURFibo bewaakt tijdige evaluatie en herziening.

4.3 Details Normenkader informatiebeveiliging mbo en Toetsingskader

Het Normenkader informatiebeveiliging mbo zoals opgenomen in dit document is compleet en direct bruikbaar. Het is gebaseerd op ISO27002:2013. Een gedetailleerde referentie van verwijzingen van en naar ISO 27002:2013 en de clusters van het Normenkader informatiebeveiliging mbo is beschikbaar in de samenwerkingsomgeving va SURFibo. Alle documenten zijn via de intranetsite van saMBO-ICT beschikbaar

4.4 Publicatie

Het Normenkader informatiebeveiliging mbo wordt in PDF vorm gepubliceerd op de websites van saMBO-ICT en Kennisnet. Het word document is opgenomen in de besloten netwerkgroep ibp in het mbo.

4.5 Referenties

Cyberdreigingsbeeld Hoger Onderwijs 2014
https://www.surf.nl/nieuws/2014/11/handvatten-om-cybersecurity-instellingen-te-verbeteren.html

Richtsnoer Beveiliging Persoonsgegevens CBP
https://cbpweb.nl/nl/richtsnoeren-beveiliging-van-persoonsgegevens-2013

ISO 27001 en 27002
https://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270012013C112014-nl-1.htm
https://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270022013-nl.htm

Bijlage 1: Samenhang ISO 27002 normenkader en HO-normenkader, inclusief nummering[3]

5	**Informatiebeveiligingsbeleid**								
5.1	**Aansturing door de directie van de informatiebeveiliging**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
5.1.1	Beleidsregels voor informatiebeveiliging (1 van 2)	1							1.1
	Beleidsregels voor informatiebeveiliging (2 van 2)	2							1.2
5.1.2	Beoordeling van het informatiebeveiligingsbeleid	3							1.3

6	**Organiseren van informatiebeveiliging**								
6.1	**Interne organisatie**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	4							1.4
6.1.2	Scheiding van taken	21							1.21
6.1.3	Contact met overheidsinstanties							1	
6.1.4	Contact met speciale belangengroepen							2	
6.1.5	Informatiebeveiliging in projectbeheer	5							1.5
6.2	**Mobiele apparatuur en telewerken**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
6.2.1	Beleid voor mobiele apparatuur (1 van 2)	6							1.6
	Beleid voor mobiele apparatuur (2 van 2)			1					3.1
6.2.2	Telewerken							3	

7	**Veilig personeel**								
7.1	**Voorafgaand aan het dienstverband**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
7.1.1	Screening		7						2.7
7.1.2	Arbeidsvoorwaarden		1						2.1
7.2	**Tijdens het dienstverband**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
7.2.1	Directieverantwoordelijkheden							4	
7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging		2						2.2
7.2.3	Disciplinaire procedure							5	
7.3	**Beëindiging en wijziging van dienstverband**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband							6	

[3] Deze bijlage is bedoeld voor auditors. Het verband tussen ISO en het MBO normenkader wordt aangegeven.. De **niet** gebruikte statements zijn in de voorlaatste kolom opgenomen.
Dus: ISO statement 5.1.1 is geplaatst in cluster 1 en is het 1e statement en krijgt dus MBO nummer 1.1
Ander voorbeeld: ISO statement 7.2.2 is geplaatst in cluster 2 en is het 2e statement en krijgt dus MBO nummer 2.2. (ISO 7.2.2 = MBO nr. 2.2)

8	Beheer van bedrijfsmiddelen								
8.1	**Verantwoordelijkheid voor bedrijfsmiddelen**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
8.1.1	Inventariseren van bedrijfsmiddelen							7	
8.1.2	Eigendom van bedrijfsmiddelen							8	
8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen							9	
8.1.4	Teruggeven van bedrijfsmiddelen							10	
8.2	**Informatieclassificatie**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
8.2.1	Classificatie van informatie	7							1.7
8.2.2	Informatie labelen	8							1.8
8.2.3	Behandelen van bedrijfsmiddelen								
8.3	**Behandelen van media**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
8.3.1	Beheer van verwijderbare media							12	
8.3.2	Verwijderen van media			2					3.2
8.3.3	Media fysiek overdragen							13	

9	Toegangsbeveiliging								
9.1	**Bedrijfseisen voor toegangsbeveiliging**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
9.1.1	Beleid voor toegangsbeveiliging					1			5.1
9.1.2	Toegang tot netwerken en netwerkdiensten					2			5.2
9.2	**Beheer van toegangsrechten van gebruikers**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
9.2.1	Registratie en afmelden van gebruikers					3			5.3
9.2.2	Gebruikers toegang verlenen					4			5.4
9.2.3	Beheren van speciale toegangsrechten					5			5.5
9.2.4	Beheer van geheime authenticatie-informatie van gebruikers					6			5.6
9.2.5	Beoordeling van toegangsrechten van gebruikers						1		6.1
9.2.6	Toegangsrechten intrekken of aanpassen		3						2.3
9.3	**Verantwoordelijkheden van gebruikers**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
9.3.1	Geheime authenticatie-informatie gebruiken					7			5.7
9.4	**Toegangsbeveiliging van systeem en toepassing**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
9.4.1	Beperking toegang tot informatie					8			5.8
9.4.2	Beveiligde inlogprocedures					9			5.9
9.4.3	Systeem voor wachtwoordbeheer							14	
9.4.4	Speciale systeemhulpmiddelen gebruiken							15	
9.4.5	Toegangsbeveiliging op programmabroncode							16	

10	Cryptografie								
10.1	**Cryptografische beheersmaatregelen**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen (1 van 2)	9							1.9
	Beleid inzake het gebruik van cryptografische beheersmaatregelen (2 van 2)	10							1.10
10.1.2	Sleutelbeheer (1 van 2)					10			5.10
	Sleutelbeheer (2 van 2)					11			5.11

11	Fysieke beveiliging en beveiliging van de omgeving								
11.1	**Beveiligde gebieden**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
11.1.1	Fysieke beveiligingszone			3					3.3
11.1.2	Fysieke toegangsbeveiliging			4					3.4
11.1.3	Kantoren, ruimten en faciliteiten beveiligen			5					3.5
11.1.4	Beschermen tegen bedreigingen van buitenaf			6					3.6
11.1.5	Werken in beveiligde gebieden			7					3.7
11.1.6	Laad- en loslocatie			8					3.8
11.2	**Apparatuur**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
11.2.1	Plaatsing en bescherming van apparatuur			9					3.9
11.2.2	Nutsvoorzieningen			10					3.10
11.2.3	Beveiliging van bekabeling			11					3.11
11.2.4	Onderhoud van apparatuur			12					3.12
11.2.5	Verwijdering van bedrijfsmiddelen	11							1.11
11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein			13					3.13
11.2.7	Veilig verwijderen of hergebruiken van apparatuur			14					3.14
11.2.8	Onbeheerde gebruikersapparatuur							17	
11.2.9	Clear desk'- en 'clear screen'-beleid		4						2.4

12	Beveiliging bedrijfsvoering								
12.1	**Bedieningsprocedures en verantwoordelijkheden**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
12.1.1	Gedocumenteerde bedieningsprocedures							18	
12.1.2	Wijzigingsbeheer				1				4.1
12.1.3	Capaciteitsbeheer							19	
12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen				2				4.2
12.2	**Bescherming tegen malware**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
12.2.1	Beheersmaatregelen tegen malware (1 van 2)				3				4.3
	Beheersmaatregelen tegen malware (2 van 2)				4				4.4
12.3	**Back-up**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
12.3.1	Back-up van informatie (1 van 2)				5				4.5
	Back-up van informatie (2 van 2)				6				4.6
12.4	**Verslaglegging en monitoren**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
12.4.1	Gebeurtenissen registreren						2		6.2
12.4.2	Beschermen van informatie in logbestanden					12			5.12
12.4.3	Logbestanden van beheerders en operators						3		6.3
12.4.4	Kloksynchronisatie			15					3.15
12.5	**Beheersing van operationele software**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
12.5.1	Software installeren op operationele systemen				7				4.7
12.6	**Beheer van technische kwetsbaarheden**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
12.6.1	Beheer van technische kwetsbaarheden				8				4.8
12.6.2	Beperkingen voor het installeren van software				9				4.9
12.7	**Overwegingen betreffende audits van informatiesystemen**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen							20	

13	Communicatiebeveiliging								
13.1	**Beheer van netwerkbeveiliging**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
13.1.1	Beheersmaatregelen voor netwerken					13			5.13
13.1.2	Beveiliging van netwerkdiensten					14			5.14
13.1.3	Scheiding in netwerken					15			5.15
13.2	**Informatietransport**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
13.2.1	Beleid en procedures voor informatietransport	12							1.12
13.2.2	Overeenkomsten over informatietransport	13							1.13
13.2.3	Elektronische berichten					16			5.16
13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst		5						2.5

14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen								
14.1	**Beveiligingseisen voor informatiesystemen**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
14.1.1	Analyse en specificatie van informatiebeveiligingseisen	14							1.14
14.1.2	Toepassingen op openbare netwerken beveiligen							21	
14.1.3	Transacties van toepassingen beschermen					17			5.17
14.2	**Beveiliging in ontwikkelings- en ondersteunende processen**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
14.2.1	Beleid voor beveiligd ontwikkelen							22	
14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen							23	
14.2.3	Technische beoordeling van toepassingen na wijzigingen besturingsplatform							24	
14.2.4	Beperkingen op wijzigingen aan softwarepakketten							25	
14.2.5	Principes voor engineering van beveiligde systemen							26	
14.2.6	Beveiligde ontwikkelomgeving				10				4.10
14.2.7	Uitbestede softwareontwikkeling						4		6.4
14.2.8	Testen van systeembeveiliging						5		6.5
14.2.9	Systeemacceptatietest						6		6.6
14.3	**Testgegevens**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
14.3.1	Bescherming van testgegevens							27	

15	Leveranciersrelaties								
15.1	**Informatiebeveiliging in leveranciersrelaties**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties							28	
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	15							1.15
15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	16							1.16
15.2	**Beheer van dienstverlening van leveranciers**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers						7		6.7
15.2.2	Beheer van veranderingen in dienstverlening van leveranciers				11				4.11

16	Beheer van informatiebeveiligingsincidenten								
16.1	**Beheer van informatiebeveiligingsincidenten en -verbeteringen**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
16.1.1	Verantwoordelijkheden en procedures	17							1.17
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	18							1.18
16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging		6						2.6
16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen				12				4.12
16.1.5	Respons op informatiebeveiligingsincidenten				13				4.13
16.1.6	Lering uit informatiebeveiligingsincidenten							29	
16.1.7	Verzamelen van bewijsmateriaal						8		6.8

17	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer								
17.1	**Informatiebeveiligingscontinuïteit**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
17.1.1	Informatiebeveiligingscontinuïteit plannen							30	
17.1.2	Informatiebeveiligingscontinuïteit implementeren				14				4.14
17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren							31	
17.2	**Redundante componenten**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten				15				4.15

18	Naleving								
18.1	**Naleving van wettelijke en contractuele eisen**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen							32	
18.1.2	Intellectuele-eigendomsrechten							33	
18.1.3	Beschermen van registraties	19							1.19
18.1.4	Privacy en bescherming van persoonsgegevens	20							1.20
18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen							34	
18.2	**Informatiebeveiligingsbeoordelingen**								
ISO nummer en naamgeving van statements		**CL1**	**CL2**	**CL3**	**CL4**	**CL5**	**CL6**	**niet**	**MBO nr.**
18.2.1	Onafhankelijke beoordeling van informatiebeveiliging							35	
18.2.2	Naleving van beveiligingsbeleid en -normen						9		6.9
18.2.3	Beoordeling van technische naleving						10		6.10

Bijlage 2: Framework informatiebeveiliging en privacy in het mbo