Toetsingskader Informatiebeveiliging cluster 1 t/m 6

versie 4.2 – oktober 2020

IBPDOC3

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

versie 4.2.1 – 12 oktober 2020

Verantwoording

In opdracht van:

Kennisnet / saMBO-ICT

Eindredactie

Leo Bakker	Kennisnet
Ludo Cuijpers	Kennisnet
Vincent Reijnen	mboRijnland
Martijn Bijleveld	saMBO-ICT

Met dank aan de leden van de werkgroep Toetsingskader 4.0

Ludo Cuijpers (voorzitter)	Kennisnet
Wim Arendse	Zadkine
Bert Barske	Drenthe College
Henk Bax	S.G. de Rooi Pannen
Martijn Bijleveld	saMBO-ICT
Bart Bosma	SURFnet
Paula Cartigny	ROC Nijmegen
Niels Dutij	Cibap
Elly Dingemanse	Kennisnet
Elke van Essen	Kien
Samantha Lejeune	Vista College
Fung Yee Poon	Aventus
Daniël Rense	Meerkring
Rene Ritzen	SURFnet
Leander Versleijen	Movare
Jurrian Wijffels	Fontys Hogescholen
Rene Zaal	Novacollege
Frits van Zadelhoff	Koning Willem I College

Update versie 4.2 (september 2020)

Fung Yee Poon	Aventus
Samantha Rodolf-Lejeune	VISTA-college
Annemarie Arnaud De Calavon	Alfa College
Wim Arendse	Grafisch Lyceum Utrecht
Roza van Cappellen	Kennisnet
Martijn Bijleveld	saMBO-ICT / Kennisnet

Sommige rechten voorbehouden

Inleiding

Het Toetsingskader Informatiebeveiliging IBPDOC3 is een centraal document in de hele aanpak rond informatiebeveiliging en privacy in het mbo. Het vormt het hart van hiervan omdat het een algemeen geaccepteerd kader biedt om de maatregelen rond ibp te toetsen en zo goed mogelijk te waarderen. Het is bedoeld om self-assessment in het onderwijs voor ibp te faciliteren en vormt een opstap om verdere auditing te gaan doen. Kenmerkend voor het vakgebied auditing is dat een onderzoek plaatsvindt ten opzichte van een eerder opgesteld en afgestemd normenkader. Zonder normenkader is een onderzoek feitelijk geen audit. Het kader ligt ook ten grondslag aan de Benchmarks ibp in het mbo die de afgelopen jaren zijn gehouden en die een goed beeld geven van de ontwikkelingen die de sector op dit gebied doormaakt.
Het toetsingskader is al in 2015 vanuit het programma 'ibp in het mbo' ontwikkeld om de maatregelen op het gebied van informatiebeveiliging en privacy te standaardiseren. Het was destijds afgeleid van het vergelijkbaar kader in het hoger onderwijs en werd ook wel het kader **MBOaudit** genoemd. Het kader is opgenomen in het Framework ibp in het mbo, dat een complete set van normen, kaders, handreikingen, formats en modellen bevat die kunnen worden ingezet voor het verbeteren van ibp in het mbo.
MBOaudit hanteert het generieke internationale normenkader voor informatiebeveiliging ISO27001 en de daarvan afgeleide set van best practices ISO 27002. In de literatuur is dit normenkader bekend onder de titel "Code voor Informatiebeveiliging". Het operationele toetsingskader van de **MBOaudit** is afgeleid van ISO 27002. Dit normenkader is verrijkt tot een toetsingskader door er bewijslast aan toe te voegen.

Het normenkader is voor het onderwijs ingedeeld in zes clusters, gebaseerd op thema's:

Cluster 1: Beleid en organisatie	24 statements
Cluster 2: Personeel, studenten en gasten	10 statements
Cluster 3: Ruimten en apparatuur	20 statements
Cluster 4: Continuïteit	17 statements
Cluster 5: Toegangsbeveiliging en integriteit	19 statements
Cluster 6: Controle en logging	11 statements

Dat maakt totaal ***101*** statements. De clustering is gebaseerd op een logische indeling die goed bruikbaar is voor het mbo- onderwijs. Per cluster zijn ook kwaliteitsaspecten af te leiden.

Schematische samenvatting

Cluster	Onderwerpen (o.a.)	Kwaliteitsaspecten	Betrokkenen
1. Beleid en Organisatie 24 statements	Informatiebeveiligingsbeleid Classificatie Inrichten beheer	• Beschikbaarheid • Integriteit • Vertrouwelijkheid • Controleerbaarheid	College van Bestuur Directeuren
2. Personeel, studenten en gasten 10 statements	Informatiebeveiligingsbeleid Aanvullingen arbeidsovereenkomst Scholing en bewustwording	• Integriteit • Vertrouwelijkheid	College van Bestuur Dienst HR Ondernemingsraad
3. Ruimte en Apparatuur 20 statements	Beveiligen van hardware, devices en bekabeling	• Beschikbaarheid • Integriteit	College van Bestuur ict dienst of afdeling
4. Continuïteit 17 statements	Anti virussen, back up, bedrijf continuïteit planning	• Beschikbaarheid	College van Bestuur ict dienst of afdeling Functioneel beheer
5. Toegangsbeveiliging en Integriteit 19 statements	Gebruikersbeheer, wachtwoorden, online transacties, sleutelbeheer, validatie	• Integriteit • Vertrouwelijkheid	College van Bestuur Functioneel beheer ict dienst of afdeling

6. Controle en logging 11 statements	Systeemacceptatie, loggen van gegevens, registreren van storingen, toetsen beleid	• Controleerbaarheid	College van Bestuur Stafmedewerker informatiebeveiliging Kwaliteitszorg

Bewijsvoering ingedeeld op 5 volwassenheidsniveaus

Het **Capability Maturity Model** is een model dat aangeeft op welk volwassenheidsniveau de informatiebeveiliging van een organisatie zit. Door ervaring in het gebruik is gebleken dat dit model op diverse processen in de organisatie toepasbaar is, ook op informatiebeveiligingsbeleid.

Volwassenheidsniveau 1 *Ad hoc*	Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen. ▪ Geen of beperkte controls geïmplementeerd. ▪ Niet of ad-hoc uitgevoerd. ▪ Niet /deels gedocumenteerd. ▪ Wijze van uitvoering afhankelijk van individu.
Volwassenheidsniveau 2 *Opzet, bestaan en beperkte werking*	Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd. ▪ Control is geïmplementeerd. ▪ Uitvoering is consistent en standaard. ▪ Informeel en grotendeels gedocumenteerd.
Volwassenheidsniveau 3 *Uitgebreide werking*	Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst. ▪ Control gedefinieerd o.b.v. risico assessment. ▪ Gedocumenteerd en geformaliseerd. ▪ Verantwoordelijkheden en taken eenduidig toegewezen. ▪ Opzet, bestaan en effectieve werking aantoonbaar. ▪ Rapportage van uitvoering van beheersingsmaatregel aan management. ▪ Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie. ▪ De toetsing toont aan dat de control effectief is.
Volwassenheidsniveau 4 *PDCA*	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd. ▪ Periodieke (control) evaluatie en opvolging vindt plaats. ▪ Evaluatie is gedocumenteerd en geformaliseerd. ▪ Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks. ▪ Rapportage van de evaluatie aan management.
Volwassenheidsniveau 5 *Externe goedkeurende verklaring*	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering. ▪ Continu evalueren van de beheersingsmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit Self-assessment, gap en root cause analyses. ▪ De getroffen beheersingsmaatregelen worden gebenchmarkt en zijn 'Best Practice' in vergelijking met andere organisaties. ▪ Real time monitoring. ▪ Inzet automated tooling.

In het toetsingskader zijn alleen de bewijslast voor de niveaus 2 en 3 beschreven. Voor niveau 1 is dat niet nodig (adhoc, er is geen bewijslast voor dit laagste niveau). Voor niveau 4 geldt dat dit hetzelfde is als niveau 3 maar dan geborgd in een jaarlijkse pdca-cyclus. Niveau 5 is gelijk aan niveau 4 maar dan voorzien van een externe verklaring. Die laatste twee behoeven dus geen beschrijving op statement niveau. Samengevat:

1 **Niveau 1**: Adhoc
② **Niveau 2**: Opzet, bestaan en beperkte werking
③ **Niveau 3**: Werking
4 **Niveau 4**: PDCA-cyclus
5 **Niveau 5:** Externe goedkeurende verklaring

Toetsingskader Informatiebeveiliging, versie 4

De update 4.0 van het toetsingskader kwam tot stand in de zomer van 2019. Op basis van deze versie is de Benchmark IBP/E 2019 uitgevoerd, gevolgd door de peer review. Bij deze update werden de volgende uitgangspunten gehanteerd:

- Bijna hele normenkader van ISO 27002;
- Bruikbaar voor alle onderwijssoorten, dus PO/VO, MBO en HO;
- Het nieuwe Toetsingskader IB maakt ook gebruik van bewijsvoering (evidence) op basis van interviews, waarneming ter plaatse en re-performance (doorlopen van een vastgesteld proces);
- Bewijslast (evidence) is gebaseerd op documenten, interviews, waarneming ter plaatse en re-performance (uitvoeren van een proces).

Voorbeeld bewijslast: Documenten

Cluster:	**1 Beleid en Organisatie**
Toetsingskader 4.0 nummer: 1.1	ISO-27002 nummer: 5.1.1
Controledoelstelling: Beleidsregels voor informatiebeveiliging Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het College van Bestuur.	

> Overleg het IBP-beleid

Voorbeeld bewijslast: Interview

Cluster:	**2 Personeel, studenten en gasten**
Toetsingskader 4.0 nummer: 2.4	ISO-27002 nummer: 11.2.9
Controledoelstelling: '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.	

> Interview het hoofd Personeelszaken betreffende clear desk en clear screen beleid. Maak hier een verslag van dat door het hoofd Personeelszaken wordt ondertekend

Voorbeeld bewijslast: Waarneming ter plaatse

Cluster:	3 Ruimten en apparatuur
Toetsingskader 4.0 nummer: 3.3	ISO-27002 nummer: 11.1.1
Controledoelstelling: Fysieke beveiligingszone Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	

> Door waarneming op de onderwijslocatie vastgesteld:

Zone	Omschrijving	Betrokken	Type beveiliging	Voorbeeld
1	Openbaar	Eenieder	geen	Trottoir
2	Enige beperking	Medewerkers, deelnemers en relaties	+ cameratoezicht	Parkeerterrein
3	Beperking	Medewerkers en deelnemers	+ algemeen pasje	Gebouw
4	Controle	Medewerkers met functie	+ pasje op functie	Administratie
5	Controle en logging	Medewerkers op naam	+ pasje op naam en logging	Examenopslag MER / SER

Voorbeeld bewijslast: Re performance

Cluster:	4 Continuïteit
Toetsingskader 4.0 nummer: 4.	ISO-27002 nummer: 8.
Controledoelstelling: 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.	

> Bedenk een fictief maar realistisch ernstig datalek en neem de hele procedure door die daarop volgt. Kijk ook mee in TOPdesk, Smile, e.d. Stop het proces als er een melding aan de AP moet worden gedaan.
Leg dit vast in een verslag en leg dit voor ter ondertekening aan de verantwoordelijke.

Update Toetsingskader Informatiebeveiliging versie 4.2

Naar aanleiding van feedback vanuit de Benchmark IBP/E 2019 en de daarna uitgevoerde peer review heeft de Regiegroep IBP besloten een beperkte update van het toetsingskader door te voeren. Doel hiervan was:

- enkele (nieuwe) statements te beoordelen op relevantie
- de toelichting van de statements hier en daar te verduidelijken en strikter te baseren op de ISO 27002 teksten
- de beschrijvingen van de bewijslast waar nodig aan te passen, zodat deze richtinggevend is en niet te letterlijk geïnterpreteerd wordt
- duidelijk markeren dat een statement deel uitmaakt van het gemeenschappelijk normenkader Privacy en/of Examinering en
- een toelichting waarom het statement is opgenomen in dat gemeenschappelijke normenkader.

Medio 2020 heeft een werkgroep het toetsingskader beoordeeld op bovenstaande punten en de wijzigingen verwerkt in deze update versie 4.2, die in september 2020 is vastgesteld door de Regiegroep IBP. Er zijn in deze update 7 statements vervallen en er is een statement verplaatst naar een ander cluster. Het totale aantal statements bedraagt nu 101.

Er zijn drie IB-statements toegevoegd aan het gemeenschappelijke normenkader privacy (1.5, 4.13 en 5.27) en twee statements zijn toegevoegd aan het gemeenschappelijke normenkader Examinering (1.1 en 1.8).
In de vorige versie was per statement een beoordelingsformulier opgenomen. Om de omvang van het document te beperken is ervoor gekozen om dit beoordelingsformulier slechts eenmaal te tonen.

Spreadsheet

Alle statements IB zijn bij elkaar gebracht in een spreadsheet samen met de aanvullende clusters Privacy en Examinering. Dit spreadsheet is voor velen heel hanteerbaar om het self assessment te ondersteunen. Het spreadsheet is opgenomen in het Framework 2.0

Samenhang met andere documenten

De samenhang tussen alle documenten, zoals die geproduceerd worden in opdracht van de *Regiegroep IBP in het mbo*, wordt beschreven in de Roadmap[1] en in de **Aanpak IBP in het mbo**.
De verantwoording van dit document is terug te vinden in:
-Verantwoordingsdocument informatiebeveiliging en privacy in het mbo onderwijs (IBPDOC1): met name de verantwoording waarom informatiebeveiliging en privacy beleid in de MBO sector wordt geïmplementeerd;
-Normenkader informatiebeveiliging mbo (IBPDOC2A): met name de onderbouwing van het toetsingskader en de verantwoording naar de externe toezichthouders.

Het toetsingskader gebruiken

Dit document is onderdeel van het Framework IBP in het mbo, dat in 2015 is opgeleverd onder verantwoording van de Taskforce IBP (Programma Informatiebeveiliging (IB) en Privacy in het mbo) en nu wordt onderhouden door de Regiegroep IBP in het mbo.

Het document kan op een vele manieren worden gebruikt:

1. **Nulmeting** voor de mbo instelling. Deze meting geeft niet alleen een volwassenheidsniveau aan, op een schaal van 1 (onvolwassen) tot 5 (droom scenario), maar ook de onderdelen waar duidelijk (bewijsbaar) onder de maat wordt gepresteerd.
2. **Baseline voor de mbo sector**. Al dan niet in overleg met OC&W kan een minimaal wenselijk niveau worden bepaald waarbij ook rekening wordt gehouden met aanvullende speerpunten, zoals examinering. Als sector hebben we aangegeven dat niveau 2 de baseline is (minimum niveau voor alle statements) en dat niveau 3 het ambitieniveau is dat in 2020 bereikt zou moeten worden. Voor sommige statements bijvoorbeeld in het kader van examinering zou al eerder een hoger niveau (3 of zelf 4) gewenst zijn.
3. **Baseline en ambitie voor de mbo instelling.** Op basis van de uitkomsten van de nulmeting en de baseline en ambitie niveaus voor de mbo sector kan de mbo instelling haar eigen baseline en ambitie bepalen, die hoger (ambitieuzer) of lager (er moet nog een inhaalslag gemaakt worden) kan worden bepaald.
4. **Benchmark** voor de mbo sector. In het najaar 2020 krijgen alle mbo instellingen weer de mogelijkheid om hier aan deel te nemen. Op basis van de uitkomsten van deze benchmark kunnen door Kennisnet of saMBO-ICT nieuwe initiatieven worden ontplooid.
5. **Aanvulling audit kwaliteitszorg.** Kwaliteitszorg moet kunnen aantonen dat digitale examens voldoen aan allerlei eisen zoals die door de sector in nauw overleg met de Inspectie zijn vastgesteld. Dit toetsingskader toont aan met hard bewijs of een mbo instelling al dan niet voldoet aan de gestelde eisen.
6. **Input accountsverklaring jaarrekening.** Het komt steeds vaker voor dat accountantskantoren inzicht willen hebben in de informatiebeveiliging van een mbo instelling. Dit toetsingskader is afgeleid van een internationaal vastgesteld normenkader (ISO 27001-27002) en dus voor een accountant acceptabel.
7. **Privacy beleid aanzet.** Een aantal overlappende statements verzorgen input voor het privacy beleid dat door een mbo-instelling vervolgens vorm kan worden gegeven.
8. **Examinering,** dat geldt ook voor examinering, een set overlappende statements uit het IB-kader kunnen aanleiding geven om het examen beleid nader te overwegen.

[1] Mbo roadmap informatie beveiligingsbeleid voor de mbo sector (IBPDOC5)

Beoordelingsformulier

Statement:	
Auditor(s):	
Methode van beoordeling:	
Documentatie:	
Interview:	
Waarneming ter plaatse:	
Re-performance:	
Goedkeuring van de beoordeling (naam en datum)**:**	
Referenties:	
Bevindingen opzet en bestaan (niveau 2)	
Bevinding: **Aanbeveling:**	
Bevindingen werking (niveau 3)	
Bevinding: **Aanbeveling:**	
Bevindingen PDCA (niveau 4)	
Bevinding: **Aanbeveling:**	
Conclusie:	**Volwassenheids-niveau** **X**

Index clusters

1. Beleid en organisatie

Nr.	ISO27002	Statement
1.1	5.1.1	Beleidsregels voor informatiebeveiliging
1.2	*vervallen*	
1.3	5.1.2	Beoordeling van het Informatiebeveiligingsbeleid
1.4	6.1.1	Taken en verantwoordelijkheden informatiebeveiliging
1.5	6.1.5	Informatiebeveiliging in projectbeheer
1.6	6.2.1	Beleid voor mobiele apparatuur
1.7	8.2.1	Classificatie van informatie
1.8	8.2.2	Informatie labelen
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen
1.10	*vervallen*	
1.11	11.2.5	Verwijdering van bedrijfsmiddelen
1.12	*vervallen*	
1.13	13.2.2	Overeenkomsten over informatietransport
1.14	14.1.1	Analyse en specificatie van informatiebeveiligingseisen
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie
1.17	16.1.1	Verantwoordelijkheden en procedures
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen
1.19	18.1.3	Beschermen van registraties
1.20	18.1.4	Privacy en bescherming van persoonsgegevens
1.21	6.1.2	Scheiding van taken
1.22	6.1.3	Contact met overheidsinstanties
1.23	6.1.4	Contact met speciale belangengroepen
1.24	8.2.3	Behandelen van bedrijfsmiddelen
1.25	18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen
1.26	18.1.2	Intellectuele eigendomsrechten
1.27	18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Terug naar index clusters

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**1**	**Beleid en organisatie**	**P**	**E**	AVG art. 24
Statement	**1.1**	**Beleidsregels voor informatiebeveiliging**			ISO 5.1.1

Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.

Toelichting
De organisatie heeft informatiebeveiligingsbeleid gedefinieerd dat is goedgekeurd door het CVB en de OR. Dit beleid beschrijft de aanpak van de organisatie om haar doelstellingen te bereiken op het gebied van informatiebeveiliging. De beleidsregels omvatten eisen die voortkomen uit de strategische doelstellingen van de organisatie, wet- en regelgeving en mogelijke bedreigingen op het gebied van informatiebeveiliging.

Het informatiebeveiligingsbeleid gaat in op:
-de doelstellingen en principes van informatiebeveiliging
-de toekenning van verantwoordelijkheden voor informatiebeveiligingsbeheer
-de processen voor het behandelen van incidenten

Het informatiebeveiligingsbeleid bestaat verder uit specifieke beleidsregels, onder meer op het gebied van:
-toegangsbeveiliging
-classificatie van informatie
-fysieke/omgevingsbeveiliging
-back-up
-bescherming tegen malware
-'clear desk' en 'clear screen'
-mobiele apparatuur en telewerken

Het informatiebeveiligingsbeleid wordt gevormd door de (samenhangende) combinatie van beleidsplan(nen), beleidsregels en/of richtlijnen.

Privacy en Examinering
Informatiebeveiliging is een belangrijke randvoorwaarde voor bescherming van de privacy van betrokkenen. Daarnaast is het een voorwaarde voor het borgen van de vertrouwelijkheid van de examinering. Een en ander moet tot uitdrukking komen in de doelstellingen, verantwoordelijkheden en processen die de organisatie daarvoor heeft ingericht. Een compleet en actueel informatiebeveiligings- en privacybeleid (IBP) is daarvoor een belangrijke voorwaarde.

Bewijsvoering
Er is beleid op het gebied van Informatiebeveiliging (IB) waarbinnen de doelstellingen en de governance zijn beschreven en dat is uitgewerkt in specifieke beleidsregels. Het beleid is vastgesteld door het CvB en goedgekeurd door de OR. Omdat er een relatie is tussen Privacy (P) en IB, is dit beleid bij voorkeur gekoppeld met beleid op het gebied van privacy, mogelijk in één IBP-beleid.

2 Overleg het IBP-beleid dat goedgekeurd is door het CvB en de OR.

3 Overleg een bewijsstuk dat het IBP-beleid breed is gecommuniceerd binnen de organisatie, bijvoorbeeld door een printscreen van een intranetpagina.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)
Zie ook	1.20

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**1**	**Beleid en organisatie**			AVG art. 24
Statement	**1.3**	**Beoordeling van het Informatiebeveiligingsbeleid**			ISO 5.1.2

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.

Toelichting
Het IBP-beleid (de combinatie van samenhangende IBP-documenten) wordt minimaal één keer per jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. Belangrijke wijzigingen zijn bijvoorbeeld een (de)fusie of samenwerking met nieuwe ICT-dienstenleverancier. Het functioneren van de informatiebeveiliging wordt jaarlijks gerapporteerd aan het bestuur en de OR. Elk onderdeel van het beleid heeft een eigenaar die verantwoordelijk is voor deze doorontwikkeling, beoordeling en evaluatie van de beleidsregels.

Bewijsvoering
Het IBP-beleid is onderdeel van de jaarplancyclus en/of er is periodiek overleg over IBP-bevindingen met het CvB of IBP-portefeuillehouder. Een en ander leidt tot aanpassingen van het beleid, aantoonbaar door bijvoorbeeld versiebeheer.

2 Overleg het IBP-beleid, voorzien van versiebeheer, dat goedgekeurd is door het CvB en de OR.

3 Overleg een document waaruit blijkt dat onderdelen van het IBP-beleid in het vorige jaar zijn geëvalueerd.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)

Toetsingskader informatiebeveiliging					
Cluster	**1**	**Beleid en organisatie**			AVG art. 24
Statement	**1.4**	**Taken en verantwoordelijkheden informatiebeveiliging**			ISO 6.1.1
Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.					
Toelichting Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd en gedocumenteerd als onderdeel van het IBP-beleid. Dat betekent dat voor belangrijke processen als het beheren van de netwerkinfrastructuur, het beheren van toegangsrechten of het maken van back-ups de (eind)verantwoordelijkheden zijn belegd en gedocumenteerd, in overeenstemming met het beleid.					
Bewijsvoering Het IBP-beleid omvat de governance van de informatiebeveiliging, met een beschrijving van alle functies en rollen, bijvoorbeeld aan de hand van het 3-lines of defence model.					
2 Overleg het IBP-beleid met betrekking tot de governance, waarin functies, rollen en verantwoordelijkheden duidelijk zijn beschreven.					
3 Overleg een overzicht met namen, functies en rollen en check voor enkele medewerkers, bijvoorbeeld door middel van een interview, of deze hun taken op basis van dit overzicht/beleid uitvoeren.					
Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)				
Zie ook	1.1				

Toetsingskader informatiebeveiliging				
Cluster	**1**	**Beleid en organisatie**	**P**	AVG art. 25
Statement	**1.5**	**Informatiebeveiliging in projectbeheer**		ISO 6.1.5

Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.

Toelichting
Informatiebeveiliging moet geïntegreerd zijn in alle projecten van de organisatie en niet alleen bij ICT. Dit zorgt ervoor dat informatiebeveiligingsrisico's tijdig worden geïdentificeerd en opgepakt als deel van een project. Deze IB(P) toets dient een vast onderdeel te zijn van elke projectinitiatie. Dit geldt in het algemeen voor elk project ongeacht het karakter, bijv. een project voor een proces voor kernactiviteiten, ICT, facilitymanagement en andere ondersteunende processen.

Privacy
Privacy by design is een belangrijk uitgangspunt van de AVG en het is daarom belangrijk om bij de initiatie van projecten de check op privacyaspecten mee te nemen.

Bewijsvoering
IBP is een vast onderdeel van de projectinitiatie en projectdocumentatie. Informatiebeveiliging en Privacy in projectbeheer wordt getoetst d.m.v. een BIV-classificatie, een gegevensverwerkingsanalyse. Voor gegevensverwerkingen die op basis daarvan een hoog risico voor de betrokkenen inhouden wordt een DPIA uitgevoerd.

2 Overleg een in de organisatie gehanteerd project- of DPIA-format waarin een IB-check is opgenomen op basis van de BIV-classificatie.

3 Overleg een overzicht van uitgevoerde gegevensverwerkingsanalyses en/of DPIA's waaruit blijkt dat dit een vast onderdeel van projectbeheer is.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6) Handreiking DPIA in het mbo (IBPDOC38)

Toetsingskader informatiebeveiliging				
Cluster	**1**	**Beleid en organisatie**	**P**	AVG art. 24
Statement	**1.6**	**Beleid voor mobiele apparatuur**		ISO 6.2.1

Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.

Toelichting
Er moet beleid worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren. Het beleid voor mobiele apparatuur moet rekening houden met de risico's die het werken met mobiele apparatuur in onbeschermde omgevingen, zoals de thuiswerkplek met zich mee kan brengen.

Privacy
Er worden veel persoonsgegevens verwerkt op mobiele apparatuur, ook in de thuissituatie. In het beleid moet de beveiliging van deze toepassingen en devices speciale aandacht krijgen.

Bewijsvoering
Het IBP-beleid bevat richtlijnen met betrekking tot het werken met mobiele apparatuur.

2 Overleg de richtlijn(en) met betrekking tot het werken met mobiele apparatuur.

3 Overleg een document waaruit blijkt dat medewerkers in kennis worden gesteld van de richtlijn Mobiele apparatuur.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)

Toetsingskader informatiebeveiliging				
Cluster	**1**	**Beleid en organisatie**	**P**	AVG art. 24
Statement	**1.7**	**Classificatie van informatie**		ISO 8.2.1

Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.

Toelichting
Classificatie van informatie geeft een inschatting van de gevoeligheid en het belang van de data om tot een juiste mate van beveiliging te komen. Niet alle data zijn even vertrouwelijk of moeten bij een incident even snel weer beschikbaar te zijn. Het is belangrijk om een passende mate van bescherming in te regelen; classificatie van informatie is een voorwaarde om daarbij de goede afwegingen te maken. Er is een beleid waarin de uitgangspunten van de (BIV-)classificatie worden beschreven. De classificatie wordt op Laag, Midden en Hoog niveau beschreven. De beheersmaatregelen worden eveneens op deze schaalverdeling beschreven.

Privacy
De AVG eist dat de organisatie in control is op het gebied van de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens. De (BIV-)classificatie is belangrijk voor het bepalen van de te nemen maatregelen om de privacy van betrokkenen te beschermen.

Bewijsvoering
Het IBP-beleid bevat een richtlijn met betrekking tot een "Classificatiemodel". Hiervoor wordt bijvoorbeeld het ROSA-classificatiemodel gebruikt.

2 Overleg de richtlijn met betrekking tot het classificatiemodel.

3 Overleg een document waarin medewerkers voor wie dit relevant is, in kennis worden gesteld van het bestaan van de richtlijn "Classificatiemodel" en de impact die dat heeft op hun werkzaamheden.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6) Certificeringsschema IBP ROSA (IBPDOC19)

Toetsingskader informatiebeveiliging					
Cluster	**1**	**Beleid en organisatie**	**P**	**E**	AVG art. 30
Statement	**1.8**	**Informatie labelen**			ISO 8.2.2

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.

Toelichting
Gegevens moeten na classificatie worden gelabeld volgens het binnen de organisatie gebruikte classificatieschema (zie 1.7). Dit geldt voor hardware en software (gegevensbestanden). Labelen kan in fysieke vorm (bijv. sticker op een verwijderbare media) of elektronisch (bijv. een watermerk in een spreadsheet).

Privacy
Voor een adequate bescherming van (bijzondere) persoonsgegevens is het belangrijk om deze goed als zodanig te kunnen identificeren. Goed bijgewerkte dataregisters spelen een belangrijke rol daarbij.

Examinering
Labeling speelt een cruciale rol in de borging van de beschikbaarheid, integriteit en vertrouwelijkheid van examens.

Bewijsvoering
Classificatie en labeling van informatie vindt aantoonbaar plaats op basis van ten minste de vastgestelde dataregisters (=register voor verwerkingsactiviteiten, globale autorisatie en BIV-classificatie). Eventueel aanvullend bijvoorbeeld een security architectuur document en/of het gebruik van een ‘stempel’ vertrouwelijk.

2 Overleg de binnen de organisatie vastgestelde dataregisters en/of andere documentatie waarin de richtlijnen voor classificatie en labeling worden beschreven.

3 Onderbouw aan de hand van publicaties/werkinstructies dat medewerkers worden geïnformeerd dan wel geïnstrueerd over classificatie en labeling van informatie, zoals bepaald in onder andere de dataregisters.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6) Format dataregisters in het mbo (IBPDOC20)
Zie ook	1.7, 1.24

Toetsingskader informatiebeveiliging					
Cluster	**1**	**Beleid en organisatie**	**P**	**E**	AVG art. 32
Statement	**1.9**	**Beleid inzake het gebruik van cryptografische beheersmaatregelen**			ISO 10.1.1

Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.

Toelichting
Er is beleid ontwikkeld en geïmplementeerd voor het toepassen van encryptie (versleuteling) voor de bescherming van informatie. Denk daarbij aan het beschermen van de websites dmv beveiligingscertificaten (https), het digitaal ondertekenen van berichten en de encryptie van gegevens op mobiele apparatuur en verwijderbare media met technologieën zoals Bitlocker. Het beleid voorziet ook in het kunnen ontsleutelen van informatie bij verlies van de sleutel of om te kunnen voldoen aan wettelijke eisen.

Privacy en Examinering
Om in een open omgeving als een onderwijsorganisatie op een veilige manier met persoonsgegevens en/of vertrouwelijke gegevens te kunnen werken, is encryptie van deze gegevens een belangrijke voorwaarde.

Bewijsvoering
Het IBP-beleid bevat een of meerdere richtlijnen met betrekking tot de encryptie van informatie.

2 Overleg een richtlijn met betrekking tot dergelijke "cryptografische beheersmaatregelen".

3 Overleg een document waarin medewerkers in kennis worden gesteld van zo'n richtlijn met betrekking tot cryptografie, bijvoorbeeld via een printscreen van de betreffende intranetpagina. Toon aan dat cryptografische maatregelen daadwerkelijk worden toegepast, bijvoorbeeld door een printscreen die onderbouwt dat Bitlocker standaard op alle laptops is geactiveerd.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)

Toetsingskader informatiebeveiliging					
Cluster	**1**	**Beleid en organisatie**			AVG art. 24
Statement	**1.11**	**Verwijdering van bedrijfsmiddelen**			ISO 11.2.5

Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.

Toelichting
De titel 'verwijdering van bedrijfsmiddelen' kan verwarrend zijn. Hier wordt bedoeld dat er een formeel proces is voor het meenemen/lenen van bedrijfsmiddelen van de locatie, zoals apparatuur, software en/of informatie(dragers). Dit gebeurt na goedkeuring. De uitleen en de terugkeer van het bedrijfsmiddel moet worden geadministreerd.

Bewijsvoering
Het IBP-beleid bevat richtlijn(en) over het meenemen/uitlenen van apparatuur, informatie en/of software. De uitgifte en inname wordt aantoonbaar geadministreerd. Voorbeelden kunnen zijn een bruikleenovereenkomst, voor een laptop, smartphone en/of software.

2 Overleg een document waarin beschreven staat welke regels er gelden voor de uitleen/het gebruik van bedrijfsmiddelen buiten de organisatie.

3 Overleg een document waarmee wordt aangetoond dat de regels voor het gebruik van bedrijfsmiddelen breed zijn gecommuniceerd. Toon met behulp van bijvoorbeeld een printscreen van Topdesk aan dat de uitgifte en inname van dergelijke bedrijfsmiddelen wordt geregistreerd.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)

Toetsingskader informatiebeveiliging					
Cluster	**1**	**Beleid en organisatie**			AVG art. 24
Statement	**1.13**	**Overeenkomsten over informatietransport**			ISO 13.2.2
Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.					
Toelichting Er moeten overeenkomsten worden vastgesteld voor de veilige uitwisseling van informatie tussen de organisatie en externe partijen. Het gaat daarbij zowel om fysieke als digitale overdracht van gegevens. Als het hierbij om persoonsgegevens gaat dan hoort daarbij een data-uitwisselingsovereenkomst of een verwerkersovereenkomst met beveiligingsbijlage.					
Bewijsvoering In de (verwerkers)overeenkomsten zijn afspraken over de uitwisseling van informatie beschreven.					
2	Overleg de standaard verwerkersovereenkomst van de instelling waarin de afspraken over de uitwisseling van informatie beschreven zijn.				
3	Overleg de verwerkersovereenkomsten m.b.t. de kern applicaties die in gebruik zijn (SIS/HRM/FIN).				
Document	Model verwerkersovereenkomst (IBPDOC18)				

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**1**	**Beleid en organisatie**			AVG art. 35
Statement	**1.14**	**Analyse en specificatie van informatiebeveiligingseisen**			ISO 14.1.1

De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.

Toelichting
Bij de invoering van nieuwe informatiesystemen, of bij de wijziging van bestaande systemen moeten de beveiligingsmaatregelen in een vroeg stadium worden meegenomen.

Bewijsvoering
Informatiebeveiligings- en privacyaspecten worden getoetst bij belangrijke wijzigingen of inkoop/aanbesteding van informatiesystemen, door middel van inkoopvoorwaarden, een gegevensverwerkingsanalyse en/of een DPIA.

2 Overleg de inkoopvoorwaarden of het gehanteerde format voor risicobeoordeling, gegevensverwerkingsanalyse en/of DPIA met de daarin de criteria ten aanzien van informatiebeveiliging.

3 Overleg een overzicht van uitgevoerde gegevensverwerkingsanalyses en/of DPIA's.

Document	Handreiking DPIA in het mbo (IBPDOC38)

Toetsingskader informatiebeveiliging					
Cluster	**1**	**Beleid en organisatie**	**P**	**E**	AVG art. 28
Statement	**1.15**	**Opnemen van beveiligingsaspecten in leveranciersovereenkomsten**			ISO 15.1.2

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.

Toelichting
Met externe partijen die toegang hebben tot informatie van de organisatie moeten overeenkomsten worden afgesloten met betrekking tot de beveiliging van deze informatie, bijvoorbeeld in de vorm van een geheimhoudingsovereenkomst, SLA en/of een verwerkersovereenkomst.

Privacy en Examinering
Voor de bescherming van de privacy van betrokkenen en de borging van een veilig examineringsproces is het belangrijk dat externe partijen zich bewust zijn van hun verantwoordelijkheid/aansprakelijkheid en dat zij daaraan gehouden kunnen worden.

Bewijsvoering
Met leveranciers die toegang hebben tot IT-infrastructuur met bedrijfsinformatie worden informatiebeveiligings- en/of verwerkersovereenkomsten afgesloten.

2 Overleg de richtlijn en/of het modelcontract/inkoopvoorwaarden met betrekking tot externe IT-dienstverleners. Overleg daarnaast de gehanteerde model-verwerkersovereenkomsten met beveiligingsbijlagen ten behoeve van externe verwerkers.

3 Overleg een lijst van leveranciers met wie de bovengenoemde afspraken zijn overeengekomen en overleg tenminste een van die contracten ter controle. Overleg daarnaast de verwerkersovereenkomsten met beveiligingsbijlagen voor de belangrijkste externe verwerkers (tenminste SIS en HRM).

Document	Model verwerkersovereenkomst (IBPDOC18)

Toetsingskader informatiebeveiliging					
Cluster	**1**	**Beleid en organisatie**		E	AVG art. 28
Statement	**1.16**	**Toeleveringsketen van informatie- en communicatietechnologie**			ISO 15.1.3

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.

Toelichting
Met leveranciers die toegang hebben tot bedrijfsmiddelen van de organisatie (applicaties, systemen en/of gegevens) moeten in overeenkomsten eisen gesteld worden aan toeleveranciers en/of samenwerkingspartners van deze leverancier. De toeleveringsketen van informatie- en communicatietechnologie omvat eveneens dienstverlening op het gebied van 'cloud computing'.

Examinering
Veel externe aanbieders van examens maken gebruik van een netwerk van toeleveranciers, bijvoorbeeld voor de ontwikkeling van examens. Deze onderaannemers moeten werken volgens de overeengekomen beveiligingswaarborgen. Daarop moet worden toegezien en gehandhaafd.

Bewijsvoering
Het format van de generieke verwerkersovereenkomst wordt als standaard gehanteerd bij de verwerking van persoonsgegevens. Bij overige gegevensverwerkingen kan een hiervan afgeleid model worden gebruikt, waarbij tenminste de classificatie van de gegevens, de beveiligingswaarborgen en de afspraken rondom de inzet van subverwerkers zijn beschreven.

2 Overleg een document waaruit blijkt dat een standaard format voor verwerkersovereenkomsten wordt gebruikt, bijvoorbeeld IBPDOC18 van het Framework IBP.

3 Overleg een lijst van leveranciers met wie de bovengenoemde afspraken zijn overeengekomen en overleg tenminste een van die contracten ter controle. Overleg daarnaast de verwerkersovereenkomsten met beveiligingsbijlagen voor de belangrijkste externe verwerkers (tenminste SIS en HRM).

Document	Model verwerkersovereenkomst (IBPDOC18)

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**1**	**Beleid en organisatie**		E	AVG art. 33
Statement	**1.17**	**Verantwoordelijkheden en procedures**			ISO 16.1.1

Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.

Toelichting
De (management)verantwoordelijkheden en -procedures moeten zijn ingeregeld om snel en doeltreffend op informatiebeveiligingsincidenten te kunnen reageren. Het gaat hier over het beleggen van verantwoordelijkheden en het inregelen van het proces, niet over de uitvoering van het incidentrespons-proces.

Examinering
Informatiebeveiligingsincidenten met betrekking tot het proces van examineren kunnen een grote impact hebben op de organisatie, zowel intern als extern, en moeten daarom direct worden geëscaleerd naar het juiste managementniveau.

Bewijsvoering
Het IBP-beleid gaat in op de governance met betrekking tot het afhandelen van informatiebeveiligingsincidenten.

2 Overleg het onderdeel van het IBP-beleid waarin de governance omtrent informatiebeveiligingsincidenten en datalekken is vastgesteld.

3 Overleg een document waarin onderbouwd wordt dat relevante medewerkers in kennis zijn gesteld van het beleid met betrekking tot het afhandelen van informatiebeveiligingsincidenten en datalekken.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**1**	**Beleid en organisatie**	**P**	**E**	AVG art. 32, 33
Statement	**1.18**	**Rapportage van informatiebeveiligingsgebeurtenissen**			ISO 16.1.2

Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.

Toelichting
De procedures voor het tijdig rapporteren van informatiebeveiligingsincidenten zijn gedefinieerd en alle medewerkers zijn hierover geïnformeerd.

Privacy en Examinering
De impact kan aanzienlijk worden beperkt door een tijdige reactie. Een belangrijk privacy-aspect is de tijdige beoordeling/reactie op datalekken.

Bewijsvoering
De procedures voor het melden van informatiebeveiligingsincidenten zijn opgenomen in het IBP-beleid. Daarbij wordt ook ingegaan op de wijze waarop medewerkers en studenten hierover worden geïnformeerd.

2 Overleg het IBP-beleid waarin de rapportage van beveiligingsgebeurtenissen is beschreven.

3 Overleg een printscreen/rapportage van de meest recente incidenten waaruit de werking van de procedure wordt aangetoond.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)

Toetsingskader informatiebeveiliging					
Cluster	**1**	**Beleid en organisatie**	**P**	**E**	AVG art. 24
Statement	**1.19**	**Beschermen van registraties**			ISO 18.1.3
Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.					
Toelichting Om gegevens te beschermen worden richtlijnen/regels verstrekt voor het classificeren, opslaan, behandelen en verwijderen van informatie. **Privacy en Examinering** Het classificeren van informatie is een belangrijke voorwaarde om passende beschermingsniveaus en bewaartermijnen te kunnen inregelen.					
Bewijsvoering Het IBP-beleid bevat richtlijnen voor classificatie van informatie, passende bescherming en de te hanteren bewaartermijnen.					
2	Overleg de Dataregisters: Medewerker, Student en Relatie, waarin de classificatie van gegevens en de bewaartermijnen zijn opgenomen.				
3	Overleg een document/printscreen waaruit blijkt dat de bescherming van de gegevens afhankelijk is van de classificatie. Er zijn bijvoorbeeld aanvullende toegangseisen (MFA) op basis van de classificatie. Ook de bewaartermijnen worden correct gehanteerd; de bewaking hiervan is bijvoorbeeld aantoonbaar in het ontwerp van het SIS/HR ingebouwd.				
Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6) Format dataregisters in het mbo (IBPDOC20) Documentair Structuurplan MBO Raad Certificeringsschema IBP ROSA (IBPDOC19)				

Toetsingskader informatiebeveiliging				
Cluster	**1**	**Beleid en organisatie**	**P**	AVG art. 5
Statement	**1.20**	**Privacy en bescherming van persoonsgegevens**		ISO 18.1.4

Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

Toelichting
Er moet beleid worden ontwikkeld, geïmplementeerd en gecommuniceerd met betrekking tot de privacy en bescherming van persoonsgegevens, op basis van de AVG. Dit statement is de verbindende schakel tussen informatiebeveiliging en privacy.

Privacy
Bescherming van privacy wordt in samenhang met het informatiebeveiligingsbeleid geregeld, bij voorkeur in de vorm van een IBP-beleid.

Bewijsvoering
In het goedgekeurde IBP-beleid is de compliance m.b.t. privacy opgenomen.

2 Overleg het IBP-beleid dat goedgekeurd is door het CvB en de OR.

3 Overleg een bewijsstuk dat het IBP-beleid breed is gecommuniceerd binnen de organisatie, bijvoorbeeld door een printscreen van een intranetpagina.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)
Zie ook	1.1 en P1

Toetsingskader informatiebeveiliging					
Cluster	**1**	**Beleid en organisatie**			AVG art. 24
Statement	**1.21**	**Scheiding van taken**			ISO 6.1.2
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.					
Toelichting Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd. Toewijzing vindt plaats in overeenstemming met het beleid. Scheiding van taken is een methode om het risico op toevallig of opzettelijk misbruik te verminderen.					
Bewijsvoering In het IBP-beleid is de governance, met alle functies en rollen duidelijk beschreven, bijvoorbeeld aan de hand van het 3-lines of defence model.					
2	Overleg het IBP-beleid met daarin opgenomen het hoofdstuk Governance waarin alle IBP-functies en rollen duidelijk zijn beschreven en waarin het principe van scheiding van taken wordt benoemd.				
3	Overleg een ingevulde lijst met namen op basis met functies en rollen. Check middels interviews of conflicterende taken op deze manier worden voorkomen en of de aangewezen medewerkers hun taken op basis van hun rol daadwerkelijk uitvoeren.				
Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)				

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**1**	**Beleid en organisatie**			AVG art. 39
Statement	**1.22**	**Contact met overheidsinstanties**			ISO 6.1.3
Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.					
Toelichting De organisatie heeft procedures die aangeven wanneer en door wie contact moet worden opgenomen met overheidsinstanties (bijv. politie, regelgevende organen, toezichthouders zoals de AP) en hoe informatiebeveiligingsincidenten tijdig worden gerapporteerd (bijv. datalekken).					
Bewijsvoering In het IBP-beleid is de governance, met alle functies en rollen duidelijk beschreven, bijvoorbeeld aan de hand van het 3-lines of defence model.					
2	Overleg een document waarin de taken van de FG, de CISO en dergelijke rollen zijn beschreven, met name op het gebied van contacten met de overheidsinstanties.				
3	Toon aan, bijvoorbeeld aan de hand van een interview met de FG, dat deze zijn taak in het kader van contacten met overheidsinstanties correct uitvoert.				
Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)				

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**1**	**Beleid en organisatie**			AVG art. 24
Statement	**1.23**	**Contact met speciale belangengroepen**			ISO 6.1.4
Er behoren passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties te worden onderhouden.					
Toelichting Lidmaatschap van speciale belangengroepen is belangrijk om: -kennis te verbeteren over best practices en op de hoogte te blijven van relevante beveiligingsinformatie; -ervoor te zorgen dat de kennis van informatiebeveiliging actueel en volledig is. Denk daarbij aan het deelnemen aan kennisnetwerken zoals het Netwerk IBP (saMBO-ICT) en de mailinglijst SCIPR (SURF).					
Bewijsvoering Het IBP-beleid bevat een richtlijn met betrekking tot kennisdeling, lidmaatschap van kennisnetwerken en relevante mailinglists en fora.					
2	Overleg een richtlijn met betrekking tot “lidmaatschap IBP-netwerken”.				
3	Toon aan, bijvoorbeeld via een interview, dat medewerkers daadwerkelijk contacten onderhouden met en deelnemen aan relevante kennisnetwerken en belangengroepen.				
Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)				

Toetsingskader informatiebeveiliging					
Cluster	**1**	**Beleid en organisatie**			AVG art. 30
Statement	**1.24**	**Behandelen van bedrijfsmiddelen**			ISO 8.2.3
Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.					
Toelichting Voor het verwerken van informatie behoren procedures te worden opgesteld die consistent zijn met de classificatie van de informatie. Dit komt bijvoorbeeld tot uitdrukking in de toegangsbeperkingen, de bescherming van de gegevens en/of het back-upbeleid.					
Bewijsvoering Het classificatiemodel is onder andere geïmplementeerd in de dataregisters en de verwerking/bescherming van de betreffende gegevens gebeurt in lijn van deze classificatie. Er wordt bijvoorbeeld 2FA toegepast bij gegevens waarvan de vertrouwelijkheid is ingeschaald op 'hoog'.					
2 Overleg de dataregisters Medewerker, Student en Relatie (of bijvoorbeeld het classificatieschema ROSA voor niet-persoonsgegevens) waarbij op basis van de classificatie van de gegevens onderscheid wordt gemaakt in de mate van bescherming.					
3 Overleg een document/printscreen waaruit blijkt dat de bescherming van de gegevens afhankelijk is van de classificatie. Er zijn bijvoorbeeld aanvullende toegangseisen (MFA) op basis van de classificatie.					
Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6) Format dataregisters in het mbo (IBPDOC20) Certificeringsschema IBP ROSA (IBPDOC19)				
Zie ook	1.7, 1.8				

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**1**	**Beleid en organisatie**			AVG art. 30, 35
Statement	**1.25**	**Vaststellen van toepasselijke wetgeving en contractuele eisen**			ISO 18.1.1

Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.

Toelichting
De eisen die de wetgeving stelt aan de informatie en het informatiesysteem moeten duidelijk in beeld zijn en er moeten beheersmaatregelen worden ontwikkeld om aan deze eisen te kunnen voldoen. Denk daarbij aan het respecteren van intellectueel eigendom, voorgeschreven bewaartermijnen of privacywetgeving.

Bewijsvoering
Relevante wetgeving en contractuele eisen met betrekking tot informatiesystemen worden vastgelegd en vormen een vast onderdeel van projectbeheer. Privacywetgeving (principes/grondslagen vanuit de AVG) wordt beoordeeld bijvoorbeeld in een gegevensverwerkingsanalyse en zo nodig een DPIA.

2 Overleg het gehanteerde format voor projectinitiatie, waarin wetgeving en contractuele eisen zijn opgenomen. Overleg daarnaast het format DPIA.

3 Overleg tenminste een uitgevoerde DPIA waarin toegepaste wetgeving en contractuele eisen zijn meegenomen.

Document	Handreiking DPIA in het mbo (IBPDOC38)

Toetsingskader informatiebeveiliging					
Cluster	**1**	**Beleid en organisatie**			AVG art. 5
Statement	**1.26**	**Intellectuele eigendomsrechten**			ISO 18.1.2
Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen behoren passende procedures te worden geïmplementeerd.					
Toelichting Materiaal dat kan worden beschouwd als intellectueel eigendom moet worden beschermd door bijvoorbeeld: -een beleid hierover te publiceren -het materiaal gecontroleerd/centraal aan te bieden -licenties te administreren.					
Bewijsvoering Relevante wetgeving en contractuele eisen met betrekking tot intellectuele eigendomsrechten worden vastgelegd en vormen een vast onderdeel van projectbeheer.					
2	Overleg een document waarin de regels voor het gebruik van auteursrechtelijk beschermd materiaal beschreven zijn, bijvoorbeeld een ‘reglement verantwoord gebruik ICT-faciliteiten’				
3	Overleg een bewijsstuk waaruit blijkt dat de regels over intellectuele eigendomsrechten breed gecommuniceerd zijn. Een voorbeelddocument is een een printscreen van een intranetpagina hierover.				
Document	Verantwoord netwerkgebruik (IBPDOC26)				

Toetsingskader informatiebeveiliging					
Cluster	**1**	**Beleid en organisatie**			AVG art. 5
Statement	**1.27**	**Voorschriften voor het gebruik van cryptografische beheersmaatregelen**			ISO 18.1.5
Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.					
Toelichting Versleuteling moet ongedaan kunnen worden gemaakt als, bijvoorbeeld als de overheid op een wettelijke grondslag hiertoe een verzoek indient.					
Bewijsvoering Het IBP-beleid bevat een richtlijn met betrekking tot "Cryptografische beheersmaatregelen" waarin is bepaald dat informatie in speciale situaties (gebaseerd op EU-recht) moet kunnen worden ontsleuteld, alsmede de voorwaarden waaronder de versleuteling ongedaan wordt gemaakt.					
2 Overleg een richtlijn "Cryptografische beheersmaatregelen" waarin het ongedaan maken van de versleuteling is geregeld.					
3 Stel vast aan de hand van een interview en/of waarneming ter plaatse dat versleuteling ongedaan gemaakt kan worden en dat er correct wordt omgegaan met dergelijke verzoeken om informatie.					
Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)				
Zie ook:	1.9				

2. Personeel, studenten en gasten

Nr.	ISO27002	Statement
2.1	7.1.2	Arbeidsvoorwaarden
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
2.3	9.2.6	Toegangsrechten intrekken of aanpassen
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst
2.6	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging
2.7	7.1.1	Screening
2.8	6.2.2	Telewerken (thuiswerken)
2.9	7.2.3	Disciplinaire procedure
2.10	*vervallen*	
2.11	7.2.1	Directieverantwoordelijkheden

Terug naar index clusters

Toetsingskader informatiebeveiliging				
Cluster	**2**	**Personeel, studenten en gasten**	**P**	AVG art. 24
Statement	**2.1**	**Arbeidsvoorwaarden**		ISO 7.1.2

De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.

Toelichting
Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de voorwaarden te aanvaarden waarin hun verantwoordelijkheden ten aanzien van informatiebeveiliging en privacy zijn vastgelegd. Er mag een gedragscode worden gebruikt om de verantwoordelijkheden van gebruikers te beschrijven ten aanzien van vertrouwelijkheid, gegevensbescherming, ethiek, passend gebruik van voorzieningen enz.

Privacy
Bovenstaande bepalingen gelden ook ten aanzien van de bescherming van de privacy van betrokkenen.

Bewijsvoering
In de arbeidsovereenkomst of overeenkomst van opdracht is een verwijzing opgenomen naar het goedgekeurde Informatiebeveiligings- en Privacybeleid, bijvoorbeeld in de vorm van een medewerkersstatuut, reglementen of gedragscodes.

2 Overleg een format arbeidsovereenkomst en contract waarin de verwijzing naar het IBP-beleid is opgenomen.

3 Overleg een recent ondertekende (geanonimiseerde) arbeidsovereenkomst en een recent ondertekend inhuur/detacheringscontract waarin de verwijzingen zijn opgenomen naar het IBP-beleid.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)

Toetsingskader informatiebeveiliging				
Cluster	**2**	**Personeel, studenten en gasten**	**P**	AVG art. 24
Statement	**2.2**	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging**		ISO 7.2.2

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.

Toelichting
Werknemers, ingehuurd personeel en externe gebruikers behoren trainingen en regelmatige bijscholing te krijgen over de regels en procedures ten aanzien van informatiebeveiliging, bijvoorbeeld in de vorm van een introductieprogramma (on-boarding) of bewustwordingstrainingen.

Privacy
Goede training is van groot belang voor de correcte omgang met persoonsgegevens.

Bewijsvoering
Er is een awareness campagne en introductie- /scholingsprogramma opgesteld voor huidige en toekomstige medewerkers.

2 Overleg een document waar de awareness (algemeen) en de scholing (doelgroepen) in het kader van IBP is beschreven en vastgesteld.

3 Overleg het gebruikte scholingsmateriaal en/of awareness campagne en maak aannemelijk dat de doelgroep heeft deelgenomen aan de scholingen en/of bekend is met het awareness-materiaal en de doelstellingen, bijvoorbeeld aan de hand van deelnemerslijsten of enkele interviews met willekeurige medewerkers.

Document	

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**2**	**Personeel, studenten en gasten**	**P**	**E**	AVG art. 32
Statement	**2.3**	**Toegangsrechten intrekken of aanpassen**			ISO 9.2.6

De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.

Toelichting
Bij beëindiging of wijziging van een rol of functie worden de toegangsrechten beoordeeld, en indien nodig ingetrokken of gewijzigd. Een actuele autorisatiematrix is voor dit statement cruciaal.
Het gaat om fysieke en logische toegangsmiddelen (sleutels, accounts, medewerkerskaart, abonnementen).

Privacy
Aandachtspunt in relatie tot privacy (AVG) is dat medewerkers uitsluitend toegang behoren te hebben tot persoonsgegevens die uit hoofde van hun functie/rol strikt noodzakelijk zijn. Actuele en fijnmazige autorisatie is daarvoor een voorwaarde.

Examinering
Met name de vertrouwelijkheid is een belangrijk aspect voor de borging van de examinering en correcte omgang met toegangsrechten is daarvoor cruciaal.

Bewijsvoering
Er is een beleid waarbinnen het intrekken of wijzigen van toegangsrechten is geregeld.

2 Overleg het vastgestelde IBP beleid waar autorisatie- en authenticatiebeleid onderdeel van is.

3 Overleg de autorisatiematrixen en stel dmv interviews en/of waarneming ter plaatse vast dat de autorisatiematrixen en de regels mbt verwijdering van autorisaties worden toegepast. Kort verslag wordt toegevoegd.

Document	Handreiking autorisatie IBP in het mbo (IBPDOC37)

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**2**	**Personeel, studenten en gasten**	**P**	**E**	AVG art. 24
Statement	**2.4**	**'Clear desk'- en 'clear screen'-beleid**			ISO 11.2.9

Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld.

Toelichting
Ter voorkoming van opzettelijk of onopzettelijk toegang krijgen tot gevoelige informatie (papier of elektronische media), behoort deze niet onbewaakt te worden achtergelaten en in afgesloten ruimtes te worden bewaard. Op de werkplek moet meelezen en meeluisteren worden voorkomen. Onbeheerde computers behoren uitgelogd of beschermd te zijn met bijvoorbeeld schermvergrendeling. Denk bij de voorlichting ook aan het 'digitale bureaublad' dat afgeschermd dient te worden bij online overleg en presentaties.

Privacy / Examinering
Vanwege het open karakter van een schoolorganisatie in combinatie met de vertrouwelijkheid van (persoons)gegevens is naleving van het 'clear desk'- en 'clear screen'-beleid een belangrijk aandachtspunt.

Bewijsvoering
Er is een "Clear desk" en "clear screen" beleid, bijvoorbeeld in de vorm van een gedragscode. Dit beleid krijgt aandacht in de awareness campagne en wordt actief gehandhaafd.

2 Overleg het "Clear desk" en "clear screen" beleid.

3 Stel door waarneming ter plaatse vast dat het "Clear desk" en "clear screen" beleid daadwerkelijk wordt nageleefd.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)

Toetsingskader informatiebeveiliging					
Cluster	**2**	**Personeel, studenten en gasten**	**P**	**E**	AVG art. 24
Statement	**2.5**	**Vertrouwelijkheids- of geheimhoudingsovereenkomst**			ISO 13.2.4

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.

Toelichting
Om de vertrouwelijkheid van informatie te waarborgen worden juridisch afdwingbare overeenkomsten afgesloten met interne en externe werknemers en andere betrokkenen met toegang tot de informatievoorziening. Dergelijke overeenkomsten hebben ook als doel om de ondertekenaars te informeren over hun verantwoordelijkheid om informatie op een verantwoorde manier te gebruiken. Voor interne medewerkers kan ook verwezen worden naar de CAO, voor externe medewerkers en gasten dienen aparte overeenkomsten gemaakt te worden of moeten dergelijke bepalingen zijn opgenomen in de contracten.

Privacy
Voor geheimhouding kan verwezen worden naar de cao. Daarnaast kan er gebruik worden gemaakt van pre-screening, VOG en/of functioneringsgesprekken. Let op dat voor externe medewerkers en gasten aparte overeenkomsten gemaakt dienen te worden.

Examinering
Dit statement is belangrijk voor het borgen van de vertrouwelijkheid van de examens.

Bewijsvoering
Er is een vertrouwelijkheid of geheimhoudingsovereenkomst beschikbaar, mogelijk als onderdeel van een bredere overeenkomst of binnen inkoopvoorwaarden.

2 Overleg het modelcontract/format m.b.t. vertrouwelijkheid of geheimhouding dat onderdeel is van het IBP-beleid.

3 Overleg een document waaruit blijkt dat alle interne en externe medewerkers kennis hebben kunnen nemen van de vertrouwelijkheids- of geheimhoudingsovereenkomst, waarbij het voor interne medewerkers duidelijk is dat dit een aanvulling is op de arbeidsovereenkomst, bijvoorbeeld door ondertekening.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)

Toetsingskader informatiebeveiliging					
Cluster	**2**	**Personeel, studenten en gasten**			AVG art. 24
Statement	**2.6**	**Rapportage van zwakke plekken in de informatiebeveiliging**			ISO 16.1.3
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.					
Toelichting Alle gebruikers van de informatiesystemen behoren eventuele kwetsbaarheden zo snel mogelijk aan het contactpunt te rapporteren om informatiebeveiligingsincidenten te voorkomen. De procedure hiervoor is eenvoudig en toegankelijk.					
Bewijsvoering Er een Responsible disclosure beleid binnen de onderwijsinstelling.					
2 Overleg een vastgesteld beleid, bijvoorbeeld een responsible disclosure beleid, waarin beschreven staat dat medewerkers, studenten en contractanten verplicht zijn om zwakke plekken in de beveiliging direct te melden bij de daarvoor aangewezen contactpunten.					
3 Overleg een bewijsstuk, bijvoorbeeld een printscreen, waaruit blijkt dat het responsible disclosure beleid instellingsstellingsbreed is gecommuniceerd.					
Document	Responsible disclosure model mbo (IBPDOC27)				

Toetsingskader informatiebeveiliging					
Cluster	**2**	**Personeel, studenten en gasten**			AVG art. 24
Statement	**2.7**	**Screening**			ISO 7.1.1

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.

Toelichting
Kandidaten voor een dienstverband worden onderworpen aan een passende verificatie van de achtergrond waarbij rekening gehouden wordt met de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.

Bewijsvoering
Voor alle in- en externe medewerkers kan een bij de functie passende VOG worden overlegd die bij indiensttreding niet ouder was dan 6 maanden**.**

2 Overleg een model arbeidsovereenkomst/contract voor in- en externe medewerkers die toegang hebben tot gevoelige gegevens en/of bijzondere persoonsgegevens waaruit blijkt dat zij een passende VOG moeten overleggen, die niet ouder is dan 6 maanden.

3 Stel aan de hand van een interview (of waarneming ter plaatse) vast dat voor alle in- en externe medewerkers een bij de functie passende VOG kan worden overlegd die bij indiensttreding niet ouder was dan 6 maanden.

Document	

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**2**	**Personeel, studenten en gasten**		E	AVG art. 24
Statement	**2.8**	**Telewerken**			ISO 6.2.2

Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.

Toelichting
Organisaties die telewerken (extern, plaatsonafhankelijk werken) toestaan, behoren een beleid te hebben dat de voorwaarden en beperkingen hiervan definieert. Het gaat dan bijvoorbeeld om maatregelen om onbevoegde toegang tot informatie of middelen door anderen te voorkomen.

Examinering
Medewerkers die betrokken zijn bij de constructie of correctie van examenwerk en deze werkzaamheden extern (bijvoorbeeld thuis) verrichten hanteren daarvoor het thuiswerkbeleid.

Bewijsvoering
Het IBP-beleid bevat een richtlijn met betrekking tot plaatsonafhankelijk/thuiswerken. Daarin is onder meer bepaald dat medewerkers die op die manier werken met vertrouwelijke informatie (vertrouwelijkheid: hoog) gebruik dienen te maken van multi-factor authenticatie en een beveiligde verbinding.

2 Overleg een richtlijn "Thuiswerken".

3 Overleg een document waaruit blijkt dat alle medewerkers in kennis worden gesteld van de richtlijn "Thuiswerken".

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)

Toetsingskader informatiebeveiliging					
Cluster	**2**	**Personeel, studenten en gasten**			AVG art. 32
Statement	**2.9**	**Disciplinaire procedure**			ISO 7.2.3
Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.					
Toelichting De formele disciplinaire procedure moet waarborgen dat medewerkers die worden verdacht van een inbreuk op de informatiebeveiliging correct en eerlijk worden behandeld. De procedure houdt rekening met factoren zoals de aard en ernst van de inbreuk en de impact ervan op de bedrijfsvoering, of dit een eerste of herhaalde overtreding is, of de overtreder al dan niet juist getraind was, relevante wetgeving en zakelijke contracten.					
Bewijsvoering In het IBP-beleid is geregeld dat medewerkers die het IBP-beleid niet naleven op een passende wijze disciplinair worden gestraft.					
2	Overleg het beleid, zoals het IBP-beleid of het medewerkersstatuut, waarin gewezen wordt op disciplinaire maatregelen bij ernstige inbreuk op de informatiebeveiliging.				
3	Stel aan de hand van een interview vast dat de disciplinaire procedure binnen de organisatie is gecommuniceerd en dat leidinggevenden deze zo nodig (kunnen) toepassen.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**2**	**Personeel, studenten en gasten**			AVG art. 40
Statement	**2.11**	**Directieverantwoordelijkheden**			ISO 7.2.1

De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.

Toelichting

De directie moet erop toezien dat werknemers, ingehuurd personeel en externe gebruikers:

- op de juiste manier worden geïnstrueerd over hun verantwoordelijkheden op het gebied van informatiebeveiliging voordat zij toegang krijgen tot vertrouwelijke informatie;
- zich daadwerkelijk houden aan het informatiebeveiligingsbeleid;
- beschikken over de juiste houding en vaardigheden op het gebied van informatiebeveiliging en regelmatig worden bijgeschoold

Bewijsvoering

Managers, proces-eigenaren en -verantwoordelijken zien er aantoonbaar op toe dat de medewerkers voor wie zij verantwoordelijk zijn op de hoogte zijn van (voor hen relevante onderdelen) van het informatiebeveiligingsbeleid en dat beleid ook naleven. Informatiebeveiliging is bijvoorbeeld onderdeel van de cyclus van functioneren en beoordelen.

2 Overleg een document, bijvoorbeeld een format voor een functioneringsgesprek, waaruit blijkt dat informatiebeveiliging een gespreksonderwerp is.

3 Overleg een document, bijvoorbeeld een geanonimiseerd verslag van een functioneringsgesprek, waaruit blijkt dat op het gebied van informatiebeveiliging afspraken zijn gemaakt.

Zie ook:	2.2

3. Ruimten en apparatuur

Nr.	ISO27002	Statement
3.1	*vervallen*	
3.2	8.3.2	Verwijderen van media
3.3	11.1.1	Fysieke beveiligingszone
3.4	11.1.2	Fysieke toegangsbeveiliging
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen
3.6	11.1.4	Beschermen tegen bedreigingen van buitenaf
3.7	11.1.5	Werken in beveiligde gebieden
3.8	11.1.6	Laad- en loslocatie
3.9	11.2.1	Plaatsing en bescherming van apparatuur
3.10	11.2.2	Nutsvoorzieningen
3.11	11.2.3	Beveiliging van bekabeling
3.12	11.2.4	Onderhoud van apparatuur
3.13	11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur
3.15	12.4.4	Kloksynchronisatie
3.16	8.1.1	Inventariseren van bedrijfsmiddelen
3.17	8.1.2	Eigendom van bedrijfsmiddelen
3.18	8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen
3.19	8.1.4	Teruggeven van bedrijfsmiddelen
3.20	8.3.1	Beheer van verwijderbare media
3.21	8.3.3	Media fysiek overdragen
3.22	*vervallen*	

Terug naar index clusters

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 24
Statement	**3.2**	**Verwijderen van media**			ISO 8.3.2
Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.					
Toelichting Voor het beveiligd verwijderen van media (bedrijfsmiddelen/gegevensdragers) behoren formele procedures te worden vastgesteld om het risico te beperken dat vertrouwelijke informatie bij onbevoegde personen terechtkomt. De procedures zijn passend bij de gevoeligheid van de informatie.					
Bewijsvoering Het betreft hier met name het inleveren, afvoeren en vernietigen van devices zoals laptops, tablets, printers enz. De onderwijsinstelling kan dit zelf doen of een gecertificeerd bedrijf inhuren.					
2	Overleg een document of gespreksverslag waarin het verwijderen van media beschreven is.				
3	Overleg een recent certificaat van vernietiging van media. Ook kan op basis van waarneming ter plaatse de werking van de procedure worden getoetst.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 32
Statement	**3.3**	**Fysieke beveiligingszone**			ISO 11.1.1
Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.					
Toelichting Het betreft hier het classificeren/definiëren van het beveiligingsniveau van de verschillende zones binnen de onderwijslocaties. Denk daarbij aan lesruimtes, werkkamers voor docenten, serverruimtes of een examenkluis. Het gaat hier vooral om de definitie van de zones en de bouwkundige uitvoering ervan. De fysieke toegangsbeveiliging wordt geregeld in 3.4					
Bewijsvoering De beveiligingszones zijn beschreven en de locaties en de mate van beveiliging van de zones zijn passend voor de beveiligingseisen van de bedrijfsmiddelen die zich binnen de zone bevinden.					
2	Overleg een document of gespreksverslag waarin de fysieke beveiligingszones beschreven zijn.				
3	Op basis van waarneming ter plaatse wordt de werking getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 32
Statement	**3.4**	**Fysieke toegangsbeveiliging**			ISO 11.1.2
Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.					
Toelichting Statement 3.3 heeft betrekking op de definitie van beveiligingszones, dit statement betreft de fysieke beveiliging ervan, bijvoorbeeld m.b.t. toegangspasjes. Implementatierichtlijn: - Toegang tot gebieden waar vertrouwelijke informatie is wordt beperkt. - Medewerkers en gasten dragen een zichtbare identificatie. - Datum en tijdstip van binnenkomst en vertrek wordt geregistreerd. - Toegangsrechten worden regelmatig beoordeeld.					
Bewijsvoering Het betreft hier het afdwingen / de controle op de toegangsbeveiliging. Denk aan pasjes, sleutels, logboeken, etc.					
2	Overleg een document of gespreksverslag waarin de toegang tot beveiligde ruimtes is beschreven.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**		E	AVG art. 24
Statement	**3.5**	**Kantoren, ruimten en faciliteiten beveiligen**			ISO 11.1.3
Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.					
Toelichting Statement 3.4 behandelt de 'beveiligde gebieden', dit statement gaat over de beveiliging van de 'normale' werkruimten, waarbij rekening gehouden wordt met de gevoeligheid van de gegevens die er verwerkt worden. Bezoekers van de afdeling HRM worden bijvoorbeeld niet in de kantoortuin ontvangen maar in afzonderlijke spreekkamers. **Examinering** Vertrouwelijk examenmateriaal wordt in de praktijk ook veel in 'normale' werkruimten (zoals docentenwerkruimten) verwerkt, in dat verband is speciale aandacht voor dit statement vereist.					
Bewijsvoering Er zijn fysieke maatregelen getroffen, bijvoorbeeld door de situering van de werkruimtes en de fysieke toegangsbeveiliging ervan, passend bij de aard van de gegevensverwerkende activiteiten binnen de ruimte.					
2	Overleg een document of gespreksverslag waarin de beveiliging van kantoren, ruimten en faciliteiten beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 24
Statement	**3.6**	**Beschermen tegen bedreigingen van buitenaf**			ISO 11.1.4
Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.					
Toelichting Om schade door brand, overstroming en andere vormen van natuurrampen of door personen veroorzaakte rampen te kunnen vermijden, worden fysieke beschermingsmaatregelen getroffen, zoals blusinstallaties, bliksemafleiders, UPS'en etc.					
Bewijsvoering Er zijn beschermingsmaatregelen tegen bedreigingen van buitenaf genomen en deze zijn gedocumenteerd in bijvoorbeeld gebouwenrisicoanalyses, bedrijfsnoodplan etc.					
2	Overleg een document of gespreksverslag waarin de bescherming van dreigingen van buitenaf beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 32
Statement	**3.7**	**Werken in beveiligde gebieden**			ISO 11.1.5
Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.					
Toelichting Voorbeelden van beveiligde gebieden zijn een serverruimte of examenkluis. De aanwezigheid hiervan wordt alleen gedeeld met medewerkers die van het bestaan moeten weten. De ruimtes zijn fysiek beschermd en er zijn procedures aanwezig voor de toegang. Er wordt in principe altijd onder toezicht gewerkt, zowel om veiligheidsredenen als om geen gelegenheid te bieden voor kwaadaardige activiteiten.					
Bewijsvoering Er bestaan procedures om medewerkers in beveiligde gebieden, bijvoorbeeld een serverruimte, te laten werken, tijdens en buiten kantooruren.					
2	Overleg een document of gespreksverslag waarin het werken in beveiligde gebieden beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 24
Statement	**3.8**	**Laad- en loslocatie**			ISO 11.1.6
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 informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.					
Toelichting Afgiftepunten voor de ontvangst en uitgifte van goederen zijn gedefinieerd en zodanig ingericht dat onbevoegde toegang tot de goederen en/of de locatie voorkomen wordt. Denk bijvoorbeeld aan de ontvangst van examens en blanco waardepapieren, het afleveren van pakketten bij de conciërge/het servicepunt of het afhalen van afgeschreven hardware ter vernietiging.					
Bewijsvoering Afgiftepunten voor de ontvangst en uitgifte van goederen zijn aantoonbaar gedefinieerd en worden als zodanig gebruikt					
2	Overleg een document of gespreksverslag waarin de locaties voor ontvangst en uitgifte van goederen beschreven zijn.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 32
Statement	**3.9**	**Plaatsing en bescherming van apparatuur**			ISO 11.2.1
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.					
Toelichting Denk bijvoorbeeld aan de plaatsing van multifunctionals op locaties waarbij de het risico op meelezen of meenemen van documenten wordt beperkt en het zodanig plaatsen van beeldschermen dat onbevoegden niet kunnen meelezen.					
Bewijsvoering Bij de plaatsing van apparatuur wordt rekening gehouden met de bescherming tegen ongeoorloofde toegang.					
2 Overleg een document, bijvoorbeeld een PvE, of gespreksverslag waarin de plaatsing en bescherming van apparatuur beschreven is.					
3 Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.					
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 32
Statement	**3.10**	**Nutsvoorzieningen**			ISO 11.2.2
Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.					
Toelichting Denk bijvoorbeeld aan de bescherming tegen stroomuitval door een UPS-voorziening of het voorkomen van uitval van internetverbindingen door redundantie. Ook de monitoring van de capaciteit van dergelijke voorzieningen hoort hierbij.					
Bewijsvoering Er is een continuïteitsplan/calamiteitenplan waarin de bescherming/continuïteit van de ict-voorziening is beschreven. En/of er zijn inkoopvoorwaarden, SLA's en dergelijke overeenkomsten waarin de beschikbaarheid van deze nutsvoorzieningen is geregeld.					
2	Overleg een document of gespreksverslag waarin de bescherming/continuïteit van de ict-voorziening beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 32
Statement	**3.11**	**Beveiliging van bekabeling**			ISO 11.2.3
Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.					
Toelichting Bekabeling moet zoveel mogelijk onzichtbaar/ontoegankelijk worden weggewerkt. De toegang tot schakelpanelen, patchkasten en kabelruimten moet worden beveiligd. Het onbevoegd inpluggen/aansluiten van netwerkapparatuur moet zoveel mogelijk worden voorkomen (bijvoorbeeld door een multifunctional te voorzien van een vaste netwerkaansluiting in plaats van een stekker).					
Bewijsvoering Voedings- en telecommunicatiekabels zijn beschermd tegen interceptie, verstoring of schade.					
2	Overleg een document of gespreksverslag waarin de beveiliging van bekabeling beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 24
Statement	**3.12**	**Onderhoud van apparatuur**			ISO 11.2.4
Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.					
Toelichting Dit statement spreekt voor zich. Ook het afsluiten van goede servicecontracten, het strikt hanteren van afschrijvingstermijnen en het uitvoeren van software-updates draagt hieraan bij.					
Bewijsvoering Het onderhoud van apparatuur is gekoppeld aan de garantieperiode en/of afschrijvingstermijn. Onderhoud wordt alleen verricht door aangewezen gekwalificeerde interne of externe medewerkers.					
2	Overleg een document of gespreksverslag waarin het onderhoud van apparatuur beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 32
Statement	**3.13**	**Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein**			ISO 11.2.6

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.

Toelichting
Apparatuur die buiten het schoolgebouw wordt gebruikt moet goed beveiligd zijn, rekening houdend met de specifieke gebruikssituatie. Dit geldt voor de mobiele devices in bruikleen, de iPad die op het sportveld wordt gebruikt, BYOD en dergelijke. Het gaat om voorschriften ten aanzien van de beveiliging van de apparatuur zelf en om gebruiksvoorschriften; bijvoorbeeld met betrekking tot het onbeheerd achterlaten van apparatuur door de gebruiker.

Bewijsvoering
Er zijn voorzieningen, regels en procedures voor het veilig gebruik van apparatuur buiten de school, zoals bruikleenovereenkomsten en een acceptable use policy.

2 Overleg een document of gespreksverslag waarin de beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein beschreven is.

3 Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.

Zie ook	1.11, 2.8

Toetsingskader informatiebeveiliging				
Cluster	**3**	**Ruimten en apparatuur**	**P**	AVG art. 24
Statement	**3.14**	**Veilig verwijderen of hergebruiken van apparatuur**		ISO 11.2.7

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.

Toelichting
Voordat apparatuur wordt verwijderd of hergebruikt moet worden gecontroleerd of de apparatuur opslagmedia/gegevensdragers bevat. Als in de apparatuur gegevensdragers aanwezig zijn, moeten de gegevens op een zodanige manier worden gewist of overschreven dat de oorspronkelijke informatie niet meer teruggehaald kan worden. Dit betreft informatie op zowel servers, multifunctionals, pc's, beheerde/geleende notebooks, tablets, smartphones, verwijderbare media en eigen devices die worden hergebruikt of voor hergebruik worden afgevoerd.

Privacy
Opslagmedia kunnen bestanden met (gevoelige/bijzondere) persoonsgegevens bevatten, vanuit privacy-oogpunt is de controle hierop van groot belang.

Bewijsvoering
Er is een procedure/richtlijn/protocol voor het veilig verwijderen of hergebruiken van apparatuur en deze wordt correct gehanteerd.

2 Overleg een document of gespreksverslag waarin het veilig verwijderen of hergebruiken van apparatuur en verwijderbare media beschreven is.

3 Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.

Document	

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 24
Statement	**3.15**	**Kloksynchronisatie**			ISO 12.4.4
De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.					
Toelichting Dit is een voorwaarde voor correcte werking van applicaties (zeker als systemen op verschillende locaties draaien) en dit is van cruciaal belang voor de logging van (beveiligings)gebeurtenissen en de bewijsvoering van mogelijke fraude.					
Bewijsvoering Toon aan dat de kloktijden van alle in het netwerk aanwezige apparatuur gesynchroniseerd zijn.					
2	Overleg een document of gespreksverslag waarin de kloksynchronisatie beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 24
Statement	**3.16**	**Inventariseren van bedrijfsmiddelen**			ISO 8.1.1
Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.					
Toelichting Een actueel overzicht van bedrijfsmiddelen helpt om beter in control te zijn, onder andere op het gebied van het onderhouden van bedrijfsmiddelen (software en hardware) en de bescherming van gegevens. Hiervoor wordt doorgaand een configuratiedatabase (CMDB) gebruikt.					
Bewijsvoering Er is een actueel en sluitend overzicht van bedrijfsmiddelen (hardware en software), bijvoorbeeld in de vorm van een configuratiedatabase (zoals Topdesk)					
2	Overleg een document waarin het inventariseren van bedrijfsmiddelen beschreven is / wordt aangetoond.				
3	Op basis van waarneming ter plaatse wordt de werking van het document getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 24
Statement	**3.17**	**Eigendom van bedrijfsmiddelen**			ISO 8.1.2
Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.					
Toelichting De eigenaar kan een persoon of een entiteit zijn (zoals een afdeling). De eigenaar van het bedrijfsmiddel is verantwoordelijk voor het juiste beheer ervan, zoals de classificatie en autorisaties, onderhoud en verwijdering aan het einde van de levenscyclus					
Bewijsvoering Alle bedrijfsmiddelen uit het inventarisoverzicht (zie 3.16) kennen een eigenaar (bijvoorbeeld directeur ICT of directeur opleiding Zorg, etc.)					
2	Overleg een document waarin een overzicht van de bedrijfsmiddelen en de bijbehorende eigenaars/verantwoordelijken zijn vastgelegd.				
3	Op basis van waarneming ter plaatse wordt de werking van het document getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 24
Statement	**3.18**	**Aanvaardbaar gebruik van bedrijfsmiddelen**			ISO 8.1.3
Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.					
Toelichting Medewerkers en contractanten die toegang hebben tot de informatievoorziening moeten op de hoogte zijn van de informatiebeveiligingseisen en hun verantwoordelijkheden daarin.					
Bewijsvoering Binnen de organisatie zijn reglementen voor netwerkgebruik, ICT-gedragsregels of bruikleenovereenkomsten waarbinnen het aanvaardbaar gebruik wordt geregeld. Voorbeelden daarvan zijn een Acceptable Use Policy of een 'Reglement Verantwoord Netwerkgebruik'.					
2	Overleg een document waarin de regels voor het gebruik van de ICT-middelen beschreven zijn, zoals een acceptable use policy.				
3	Op basis van waarneming ter plaatse of interviews wordt de werking van het document getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document	Verantwoord netwerkgebruik (IBPDOC26)				

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 24
Statement	**3.19**	**Teruggeven van bedrijfsmiddelen**			ISO 8.1.4
Alle medewerkers en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven.					
Toelichting In de beëindigingsprocedure behoort formeel het teruggeven van alle eerder verstrekte fysieke en elektronische bedrijfsmiddelen die het eigendom zijn van of toevertrouwd zijn aan de organisatie te worden opgenomen. Voorbeelden van bedrijfsmiddelen zijn laptops, smartphones, tokens en sleutels.					
Bewijsvoering Er is een proces uitdiensttreding; het inleveren van de bedrijfsmiddelen is een onderdeel van het proces.					
2	Overleg een document, zoals een bruikleenovereenkomst waarin het teruggeven van bedrijfsmiddelen beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**3**	**Ruimten en apparatuur**			AVG art. 24
Statement	**3.20**	**Beheer van verwijderbare media**			ISO 8.3.1
Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.					
Toelichting Het gaat bijvoorbeeld om USB-sticks en externe harde schijven. In hoeverre en onder welke voorwaarden is het gebruik hiervan toegestaan. Daarbij moet rekening gehouden worden met de classificatie van de gegevens.					
Bewijsvoering Er zijn procedures en richtlijnen hoe om te gaan met verwijderbare media. Denk bijvoorbeeld aan voorschriften i.v.m. encryptie.					
2 Overleg een document of gespreksverslag waarin het regels voor verwijderbare media beschreven zijn.					
3 Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.					
Document					

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**3**	**Ruimten en apparatuur**		E	AVG art. 24
Statement	**3.21**	**Media fysiek overdragen**			ISO 8.3.3

Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of datacorruptie tijdens transport.

Toelichting
Informatie kan tijdens fysiek transport gevoelig zijn voor onbevoegde toegang, misbruik of datacorruptie, bijvoorbeeld als media/gegevnsdragers per post- of koeriersdienst worden verzonden. In deze beheersmaatregel worden onder media ook papieren documenten verstaan. Als vertrouwelijke informatie niet versleuteld is, moet aanvullende fysieke bescherming worden toegepast. Denk aan examenopgaven, waardepapieren en diploma's en ook digitale media.

Examinering
Veel examenmateriaal wordt extern aangeleverd, ook in fysieke vorm. Goede bescherming tegen onbevoegde toegang is cruciaal.

Bewijsvoering
Gevoelige informatie wordt beveiligd verstuurd, bijvoorbeeld via een koerier of aangetekende post. Digitale media worden daarbij versleuteld.

2 Overleg een richtlijn/procedure of gespreksverslag waarin de fysieke overdracht van media beschreven is.

3 Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Een kort verslag wordt toegevoegd.

Document	

4. Continuïteit

Nr.	ISO27002	Statement
4.1	12.1.2	Wijzigingsbeheer
4.2	12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen
4.3	12.2.1	Beheersmaatregelen tegen malware
4.4	*vervallen*	
4.5	12.3.1	Back-up van informatie
4.6	*vervallen*	
4.7	12.5.1	Software installeren op operationele systemen
4.8	12.6.1	Beheer van technische kwetsbaarheden
4.9	12.6.2	Beperkingen voor het installeren van software
4.10	14.2.6	Beveiligde ontwikkelomgeving
4.11	15.2.2	Beheer van veranderingen in dienstverlening van leveranciers
4.12	16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen
4.13	16.1.5	Respons op informatiebeveiligingsincidenten
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren
4.15	17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten
4.16	12.1.1	Gedocumenteerde bedieningsprocedures
4.17	12.1.3	Capaciteitsbeheer
4.18	17.1.1	Informatiebeveiligingscontinuïteit plannen
4.19	17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren

Terug naar index clusters

Toetsingskader informatiebeveiliging					
Cluster	**4**	**Continuïteit**			AVG art. 32
Statement	**4.1**	**Wijzigingsbeheer**			ISO 12.1.2
Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.					
Toelichting Onvoldoende beheersing van veranderingen aan informatieverwerkende faciliteiten en systemen kan leiden tot systeem- of beveiligingsfouten. Wijzigingen moeten daarom via een formeel proces worden aangevraagd, uitgevoerd, gedocumenteerd en worden gecommuniceerd.					
Bewijsvoering Er is een formeel proces voor wijzigingenbeheer en dit proces wordt correct gehanteerd.					
2	Overleg een document waarin het wijzigingsproces beschreven is en de verantwoordelijkheden zijn benoemd.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.				
Zie ook	5.23				

Toetsingskader informatiebeveiliging					
Cluster	**4**	**Continuïteit**			AVG art. 32
Statement	**4.2**	**Scheiding van ontwikkel-, test- en productieomgevingen**			ISO 12.1.4

Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.

Toelichting
Over het algemeen wordt de grootschalige softwareontwikkeling (SIS/HRM) uitbesteed aan externe leveranciers. Waarborgen voor dit statement worden dan geleverd door een beveiligingsbijlage bij de verwerkersovereenkomst, een SLA en/of andere contracten. Desondanks worden op kleinere schaal vaak wel in eigen beheer software-oplossingen ontwikkeld, bijvoorbeeld ten behoeve van rapportages. Dit statement is ook van toepassing op dergelijke vormen van softwareontwikkeling (rapportages niet testen met productiedata bijvoorbeeld).

Bewijsvoering
De belangrijkste applicaties (SIS/HR/FIN) maken gebruik van een OTAP-omgeving. Intern ontwikkelde toepassingen (zoals rapportages) worden ontwikkeld en getest met testdata.

2 Overleg een document of gespreksverslag waarin de scheiding van ontwikkel-, test- en productieomgevingen beschreven is.

3 Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd. Bij Saas: overleg een document waarin afspraken met leverancier over de OTAP-omgeving zijn gemaakt.

Document	

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**4**	**Continuïteit**			AVG art. 32
Statement	**4.3**	**Beheersmaatregelen tegen malware**			ISO 12.2.1
Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.					
Toelichting Er worden maatregelen getroffen voor detectie, preventie en herstel om te beschermen tegen virussen en er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten. Het betreft hier met name de aanschaf, gebruik en onderhoud van virusscanners en andere tools voor detectie van malware. Bewustzijn van de gebruikers is onderdeel van cluster 2.					
Bewijsvoering Er zijn beheersmaatregelen tegen malware beschreven, bijvoorbeeld als onderdeel van het IBP-beleid.					
2	Overleg een document of gespreksverslag waarin de beheersmaatregelen tegen malware beschreven zijn.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.				
Zie ook:	2.2				

Toetsingskader informatiebeveiliging				
Cluster	**4**	**Continuïteit**	**P**	AVG art. 32
Statement	**4.5**	**Back-up van informatie**		ISO 12.3.1

Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.

Toelichting
Er moeten back-upfaciliteiten zijn om te voorkomen dat essentiële informatie na het falen van media, bijvoorbeeld door calamiteiten, verloren gaat. Back-ups moeten bewaard worden op voldoende afstand van de hoofdlocatie, moeten goed zijn beveiligd en de herstelprocedure moet regelmatig worden getest. Bij SaaS geldt een goede verwerkersovereenkomst/bijsluiter, SLA en/of regelmatig servicemanagementoverleg als waarborg voor dit statement.

Privacy
Uit oogpunt van beschikbaarheid, integriteit verdient het regelmatig back-uppen van informatie speciale aandacht. In verband met vertrouwelijkheid dient daarbij gezorgd te worden voor beveiligde opslag.

Bewijsvoering
Er worden op basis van het back-up beleid regelmatig back-ups gemaakt, getest en deze worden veilig opgeslagen. Het terugzetten van back-ups wordt regelmatig getest.

2	Overleg een document of gespreksverslag waarin de back-up van informatie beschreven is.
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.
Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**4**	**Continuïteit**			AVG art. 32
Statement	**4.7**	**Software installeren op operationele systemen**			ISO 12.5.1
Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.					
Toelichting De beschikbaarheid van kernsystemen als het SIS en HRM moet zijn gewaarborgd en het updaten van dergelijke systemen moet volgens vastgestelde procedures gebeuren. Bij SaaS is dit in principe in de SaaS-overeenkomst geregeld. Dit betekent bijvoorbeeld dat updates pas worden uitgevoerd nadat deze zijn getest.					
Bewijsvoering Installatie/updates van software op operationele systemen gebeurt volgens een vastgestelde procedure.					
2	Overleg een document of gespreksverslag waarin software installeren op operationele systemen beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd. Bij Saas: overleg een document waarin afspraken met leverancier over het installeren van updates zijn gemaakt.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**4**	**Continuïteit**			AVG art. 24
Statement	**4.8**	**Beheer van technische kwetsbaarheden**			ISO 12.6.1

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.

Toelichting
Om snel te kunnen reageren op potentiële technische kwetsbaarheden is het belangrijk dat:
- de rollen en verantwoordelijkheden op dit gebied zijn vastgesteld;
- informatiebronnen m.b.t. kwetsbaarheden consequent worden geraadpleegd;
- er een actuele en volledige inventaris van bedrijfsmiddelen aanwezig is (zie 3.16);
- eventuele patches worden geëvalueerd en/of getest voordat ze worden geïnstalleerd.

Bewijsvoering
Beheer van kwetsbaarheden is goed georganiseerd: de rollen zijn belegd en werkzaamheden op het gebied van patch-management, hotfixes worden uitgevoerd. Een en ander is aantoonbaar via wijzigingen/incidentbeheer.

2 Overleg een document of gespreksverslag waarin het beheer van technische kwetsbaarheden beschreven is.

3 Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.

Document	

Toetsingskader informatiebeveiliging					
Cluster	**4**	**Continuïteit**			AVG art. 24
Statement	**4.9**	**Beperkingen voor het installeren van software**			ISO 12.6.2
Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.					
Toelichting Onbeheerst installeren van software op computerapparatuur kan leiden tot het introduceren van kwetsbaarheden en vervolgens tot weglekken van informatie, verlies van integriteit of andere informatiebeveiligingsincidenten, of tot schending van intellectuele-eigendomsrechten. De organisatie behoort daarom een beleid te definiëren en ten uitvoer te brengen met betrekking tot de soorten software die gebruikers mogen installeren.					
Bewijsvoering Er is een reglement voor verantwoord ICT-gebruik en/of een BYOD-beleid met bepalingen omtrent het installeren van software door de gebruiker. Deze regels zijn aantoonbaar breed gecommuniceerd binnen de organisatie.					
2	Overleg een document of gespreksverslag waarin regels of voorwaarden voor het installeren van software beschreven zijn.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.				
Document	Verantwoord netwerkgebruik (IBPDOC26)				

Toetsingskader informatiebeveiliging					
Cluster	**4**	**Continuïteit**			AVG art. 24
Statement	**4.10**	**Beveiligde ontwikkelomgeving**			ISO 14.2.6
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.					
Toelichting Ontwikkelaars van informatiesystemen moeten gebruikmaken van een beveiligde omgeving voor het ontwikkelen, integreren en testen van deze systemen, passend bij de classificatie van de gegevens die worden verwerkt. Het gaat om de set samenhangende maatregelen, onder andere op het gebied van toegangsbeveiliging, scheiding van productie en testomgeving enzovoort.					
Bewijsvoering Voor de kernsystemen (SIS, HR en FIN) is de beveiligde ontwikkelomgeving geborgd door middel van waarborgen in de contracten (VWO / SLA) met deze leveranciers.					
2	Overleg een document of gespreksverslag waarin de beveiligde ontwikkelomgeving beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.				
Zie ook	4.2				

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**4**	**Continuïteit**			AVG art. 28, 35
Statement	**4.11**	**Beheer van veranderingen in dienstverlening van leveranciers**			ISO 15.2.2

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.

Toelichting
Wijzigingen in de dienstverlening van leveranciers moeten worden beoordeeld en gedocumenteerd, bijvoorbeeld binnen het proces van wijzigingenbeheer. Het gaat onder meer om:
- veranderingen in leveranciersovereenkomsten;
- nieuwe versies of updates;
- uitbreiding van diensten/functionaliteiten.

Als de overeenkomst met een leverancier wezenlijk wordt gewijzigd, moet de nieuwe overeenkomst volledig worden beoordeeld zoals dat bij een eerste overeenkomst behoort te gebeuren.

Bewijsvoering
Binnen de organisatie is bijvoorbeeld een sourcing strategie, wordt gebruikgemaakt van supplier-scorecards, is contractmanagement ingeregeld en/of vindt regelmatig servicemanagement-overleg plaats met de belangrijkste leveranciers (SIS/HR/FIN). Bij grote wijzigingen wordt een DPIA uitgevoerd.

2 Overleg een document of gespreksverslag waarin het beheer van veranderingen in dienstverlening van leveranciers beschreven is.

3 Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.

Document	

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**4**	**Continuïteit**			AVG art. 33
Statement	**4.12**	**Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen**			ISO 16.1.4

Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.

Toelichting
Voor het melden van incidenten is een contactpunt bepaald. Het contactpunt beoordeelt elk incident en classificeert het al dan niet als informatiebeveiligingsgebeurtenis. Classificeren en prioriteren van incidenten kan helpen de impact en omvang van een incident te bepalen. Als de organisatie beschikt over een responsteam voor informatiebeveiligingsincidenten (CSIRT), kunnen de beoordeling en het besluit worden doorgestuurd naar het CSIRT voor bevestiging of herbeoordeling. Bij informatiebeveiligingsincidenten waarbij persoonsgegevens in het geding zijn moet beoordeeld worden of dit moeten worden geclassificeerd als datalek.

Bewijsvoering
Beschrijf hoe incidenten worden beoordeeld, geclassificeerd en vastgelegd (bijvoorbeeld in een registratiesysteem als TOPdesk of een GRC-tool) en hoe deze beoordeling wordt gecontroleerd.

2 Overleg een document of gespreksverslag waarin de beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen beschreven is.

3 Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.

Zie ook	1.17, 1.18

Toetsingskader informatiebeveiliging					
Cluster	**4**	**Continuïteit**	P	E	AVG art. 33
Statement	**4.13**	**Respons op informatiebeveiligingsincidenten**			ISO 16.1.5

Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.

Toelichting
Op informatiebeveiligingsincidenten moet adequaat worden gereageerd, bijvoorbeeld door:
- zo snel mogelijk na de gebeurtenis aanvullende informatie en bewijs verzamelen;
- zo nodig te escaleren naar het juiste (management)niveau;
- maatregelen te nemen om (verdere) schade te voorkomen;
- gegevens over het incident en de afhandeling ervan te documenteren.

Privacy
Informatiebeveiligingsincidenten kunnen grote gevolgen hebben voor de bescherming van de privacy van gebruikers binnen de organisatie. Als er bij ernstige incidenten persoonsgegevens in het geding zijn moet er worden gehandeld naar de procedure datalekken.

Examinering
Er is extra aandacht voor dit statement vereist in verband met de grote impact die een informatiebeveiligingsincident kan hebben op de examinering en de reputatie van de organisatie op dit gebied.

Bewijsvoering
Er is een procedure die beschrijft hoe op informatiebeveiligingsincidenten (waaronder ook datalekken) moet worden gereageerd inclusief de documentatie ervan.

2 Overleg een document waarin de respons op informatiebeveiligingsincidenten beschreven is.

3 Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.

Zie ook 1.17, 1.18, 4.12

Toetsingskader informatiebeveiliging				
Cluster	**4**	**Continuïteit**	**P**	AVG art. 32
Statement	**4.14**	**Informatiebeveiligingscontinuïteit implementeren**		ISO 17.1.2

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.

Toelichting
Ook tijdens crises en rampen dient de kwaliteit van de informatiebeveiliging te blijven functioneren. Daartoe worden maatregelen (mogelijk als onderdeel van een calamiteiten- of continuïteitsplan) getroffen om de kwaliteit van de beveiliging tijdens crisissituaties te handhaven.
Zie ook 4.18 en 4.19

Privacy
Tijdens een crisis (waaronder een cybercrisis) verdient de bescherming van persoonsgegevens extra aandacht.

Bewijsvoering
De organisatie heeft een (cyber)crisisplan, waarin wordt beschreven op welke manier op een crisis wordt geacteerd. Dit plan wordt getest en geoefend met de betrokkenen, bijvoorbeeld tijdens een (OZON)crisisoefening.

2 Overleg een document of gespreksverslag waarin de informatiebeveiligingscontinuïteit beschreven is.

3 Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd. Bevindingen (conclusies, verbetermaatregelen) van een crisisoefening daarin meenemen.

Zie ook	4.18 en 4.19

Toetsingskader informatiebeveiliging					
Cluster	**4**	**Continuïteit**		E	AVG art. 32
Statement	**4.15**	**Beschikbaarheid van informatieverwerkende faciliteiten**			ISO 17.2.1

Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.

Toelichting
Organisaties moeten de eisen voor de beschikbaarheid van informatiesystemen vaststellen door classificatie van deze systemen. Als de eisen t.a.v. beschikbaarheid hoog zijn moet het systeem mogelijk redundant worden uitgevoerd. Dit moet ook tot uitdrukking komen in de overeenkomsten met leveranciers.

Examinering
Voor (digitale) examinering is beschikbaarheid van de informatiesystemen cruciaal.

Bewijsvoering
Informatiesystemen en de daarin verwerkte gegevens zijn geclassificeerd en op basis daarvan worden eisen gesteld aan leveranciers en/of maatregelen genomen om aan de beschikbaarheidseisen te voldoen.

2 Overleg een document of gespreksverslag waarin de maatregelen om de beschikbaarheid van informatieverwerkende faciliteiten te waarborgen beschreven zijn.

3 Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.

Document	Handleiding BIV-classificatie (IBPDOC14) Format dataregisters in het mbo (IBPDOC20)

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**4**	**Continuïteit**			AVG art. 24
Statement	**4.16**	**Gedocumenteerde bedieningsprocedures**			ISO 12.1.1
Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.					
Toelichting Er moeten handleidingen en/of werkinstructies worden opgesteld voor werkzaamheden aan/met informatieverwerkende en communicatiefaciliteiten, bijvoorbeeld op het gebied van installatie en onderhoud van apparatuur, verwerking van gegevens en het maken van back-ups.					
Bewijsvoering Medewerkers die toegang krijgen tot informatieverwerkende systemen, zoals het SIS, de ELO of beheertaken voor dergelijke systemen uitvoeren krijgen daarvoor passende/toereikende instructies.					
2	Overleg een document of gespreksverslag waarin de beschikbaarheid van werkinstructies voor de bedrijfskritische systemen beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**4**	**Continuïteit**			AVG art. 32
Statement	**4.17**	**Capaciteitsbeheer**			ISO 12.1.3
Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.					
Toelichting De capaciteit van bedrijfskritische systemen wordt gemonitord en zo nodig aangepast. Daarbij wordt rekening gehouden met toekomstige verwachtingen en trends.					
Bewijsvoering De capaciteit van onder meer de stroomvoorziening, opslagcapaciteit en netwerkbandbreedte worden gemonitord en zo nodig wordt hierop ingegrepen. In overeenkomsten met leveranciers wordt hiermee rekening gehouden.					
2	Overleg een document of gespreksverslag waarin het capaciteitsbeheer beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**4**	**Continuïteit**			AVG art. 32
Statement	**4.18**	**Informatiebeveiligingscontinuïteit plannen**			ISO 17.1.1
De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen.					
Toelichting De continuïteit van de informatiebeveiliging moet zijn vastgesteld, bijvoorbeeld als onderdeel van het crisisplan of in de vorm van een bedrijfscontinuïteitsplan. De informatiebeveiliging moet in ongunstige situaties in principe blijven functioneren als in normale uitvoeringsomstandigheden.					
Bewijsvoering Voor de kernapplicaties (SIS/HR/FIN) en de kernfaciliteiten zoals internet, netwerk en nutsvoorzieningen zijn de continuïteitseisen gedefinieerd en zo mogelijk waarborgen voor continuïteit beschreven en/of ingeregeld.					
2	Overleg een document of gespreksverslag waarin het plannen van de informatiebeveiligingscontinuïteit beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.				
Zie ook	4.14 en 4.19				

Toetsingskader informatiebeveiliging					
Cluster	**4**	**Continuïteit**			AVG art. 32
Statement	**4.19**	**Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren**			ISO 17.1.3
De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.					
Toelichting Veranderingen binnen de organisatie op het gebied van procedures, processen of van technische aard kunnen leiden tot veranderingen in de eisen betreffende informatiebeveiligingscontinuïteit. De continuïteit van de informatiebeveiliging dient te worden beoordeeld tegen de achtergrond van deze veranderde eisen. Zie ook 4.14 en 4.18					
Bewijsvoering De informatiebeveiligingscontinuïteit wordt tenminste eenmaal per twee jaar beoordeeld, bijvoorbeeld door deelname en evaluatie van dit aspect in het kader van een calamiteitenoefening (bijv. OZON).					
2	Overleg een document of gespreksverslag waarin het verifiëren van de informatiebeveiligingscontinuïteit beschreven is.				
3	Op basis van waarneming ter plaatse wordt de werking van het document of gespreksverslag getoetst door de auditor. Kort verslag wordt toegevoegd.				
Zie ook	4.14 en 4.18				

5. Toegangsbeveiliging en integriteit

Nr.	ISO27002	Statement
5.1	9.1.1	Beleid voor toegangsbeveiliging
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten.
5.3	9.2.1	Registratie en afmelden van gebruikers
5.4	9.2.2	Gebruikers toegang verlenen
5.5	9.2.3	Beheren van speciale toegangsrechten
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers
5.7	9.3.1	Geheime authenticatie-informatie gebruiken
5.8	9.4.1	Beperking toegang tot informatie
5.9	9.4.2	Beveiligde inlogprocedures
5.10	10.1.2.1	Sleutelbeheer
5.11	*vervallen*	
5.12	12.4.2	Beschermen van informatie in logbestanden
5.13	*vervallen*	
5.14	13.1.2	Beveiliging van netwerkdiensten
5.15	13.1.3	Scheiding in netwerken
5.16	13.2.3	Elektronische berichten
5.17	14.1.3	Transacties van toepassingen beschermen
5.18	9.4.3	Systeem voor wachtwoordbeheer
5.19	9.4.4	Speciale systeemhulpmiddelen gebruiken
5.20	*vervallen*	
5.21	*vervallen*	
5.22	*vervallen*	
5.23	14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen
5.24	*vervallen*	
5.25	*vervallen*	
5.26	*vervallen*	
5.27	14.3.1	Bescherming van testgegevens
5.28	*vervallen*	

Terug naar index clusters

Toetsingskader informatiebeveiliging				
Cluster	**5**	**Toegangsbeveiliging en integriteit**	**P**	AVG art. 32
Statement	**5.1**	**Beleid voor toegangsbeveiliging**		ISO 9.1.1

Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.

Toelichting
Het toegangsbeleid is onderdeel van het IBP-beleid en kan in een apart document worden vastgelegd. Het toegangsbeleid is door het CvB goedgekeurd óf het is een uitvloeisel van het door het CvB vastgestelde IBP-beleid. Het beleid voor toegangsbeveiliging gaat onder meer in op:

- beveiligingseisen van de bedrijfstoepassingen;
- beleidsregels voor informatieverspreiding en -autorisatie, bijv. het 'least privilege' en 'need-to-know'-principe;
- informatiebeveiligingsniveaus en -classificatie;
- het beheer van toegangsrechten;
- eisen voor het periodiek beoordelen van toegangsrechten;
- intrekken van toegangsrechten;
- rollen met speciale toegangsrechten.

Privacy
De principes van de AVG vereisen een strikte toegangsbeveiliging op basis van het 'need to know'-principe.

Bewijsvoering
Er is vastgesteld toegangsbeleid op basis van least-privilege (alles is in principe verboden tenzij het uitdrukkelijk is toegelaten).

2 Overleg een vastgesteld autorisatie- en authenticatiebeleid.

3 Overleg een bewijsstuk waaruit blijkt dat het autorisatie en authenticatiebeleid breed is gecommuniceerd. Bijvoorbeeld een printscreen waaruit blijkt dat alle relevante gebruikers op de hoogte zijn gesteld van het autorisatie- en authenticatiebeleid.

Document	Handreiking autorisatie IBP in het mbo (IBPDOC37)
Zie ook	5.2, 5.3, 5.4, 5.5

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**5**	**Toegangsbeveiliging en integriteit**	**P**	**E**	AVG art. 32
Statement	**5.2**	**Toegang tot netwerken en netwerkdiensten**			ISO 9.1.2

Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.

Toelichting
Het gebruik van netwerken en netwerkdiensten is geregeld in beleid, dat onder andere ingaat op:

a) de netwerken en netwerkdiensten waartoe toegang wordt verleend;
b) autorisatieprocedures om vast te stellen wie toegang krijgt tot welk netwerk en welke netwerkdiensten;
c) beheersmaatregelen en -procedures om de toegang tot netwerkverbindingen en -diensten te beschermen;
d) de middelen die worden gebruikt om toegang te krijgen tot netwerken en netwerkdiensten (bijv. VPN);
e) eisen voor gebruikersauthenticatie voor de toegang tot de verschillende netwerkdiensten (eisen t.a.v. wachtwoorden, MFA);
f) monitoren van het gebruik van netwerkdiensten.

Privacy / Examinering
Ongeautoriseerde en onveilige verbindingen met netwerkdiensten vormen een bedreiging voor de privacy van betrokkenen en voor de betrouwbaarheid van het proces van examinering.

Bewijsvoering
De principes “need-to-know” en “least privilege” worden gebruikt bij het autoriseren van alle gebruikers op alle netwerken en netwerkdiensten.

2 Overleg het vastgestelde beleid voor autorisatie- en authenticatie, bijvoorbeeld het IBP-beleid of een afzonderlijke richtlijn.

3 Overleg een bewijsstuk waaruit blijkt dat autorisatie plaatsvindt op basis van het autorisatie en authenticatiebeleid. Bijvoorbeeld aan de hand van een printscreen van gebruikers, rollen en rechten.

Document	Handreiking autorisatie IBP in het mbo (IBPDOC37)
Zie ook	5.1, 5.3, 5.4, 5.5

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**5**	**Toegangsbeveiliging en integriteit**	**P**	**E**	AVG art. 5, 32
Statement	**5.3**	**Registratie en afmelden van gebruikers**			ISO 9.2.1

Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.

Toelichting
De procedure voor het beheren van gebruikersaccounts voorziet o.a. in:
- het gebruik van unieke gebruikersaccounts zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gehouden voor hun acties;
- het onmiddellijk deactiveren of verwijderen van de accounts van gebruikers die de organisatie hebben verlaten;
- het periodiek beoordelen en zo nodig verwijderen van overbodige toegangsrechten;

Privacy / Examinering
Ongeautoriseerde toegang vormt een bedreiging voor de privacy van betrokkenen en voor de betrouwbaarheid van het proces van examinering. Een goed functionerend proces voor het beheren van gebruikersaccounts/toegangsrechten is daarvoor cruciaal.

Bewijsvoering
Er is een proces voor instroom, doorstroom en uitstroom (IDU proces) ingericht, op basis waarvan de juiste autorisaties aan gebruikers worden toegekend.

2 Overleg het vastgestelde beleid voor autorisatie- en authenticatie, bijvoorbeeld het IBP-beleid of een afzonderlijke richtlijn, waarin de formele registratie- en afmeldingsprocedure is beschreven.

3 Overleg een bewijsstuk waaruit blijkt dat er volgens de IDU-proces wordt gewerkt. Bijvoorbeeld printscreen uit Topdesk.

Document	Handreiking autorisatie IBP in het mbo (IBPDOC37)
Zie ook	2.3, 5.1, 5.2, 5.4, 5.5

Toetsingskader informatiebeveiliging

REGIEGROEP IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Cluster	**5**	**Toegangsbeveiliging en integriteit**	**P**	AVG art. 5, 32
Statement	**5.4**	**Gebruikers toegang verlenen**		ISO 9.2.2

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.

Toelichting

Er is een procedure voor het toewijzen of intrekken van toegangsrechten. De procedure omvat onder andere:

- de controle dat het verleende toegangsniveau in overeenstemming is met de beleidsregels voor toegang (zie 5.1) en consistent is met andere eisen zoals een scheiding van taken (zie 1.21);
- bijhouden van een centraal overzicht van toegangsrechten die aan accounts zijn toegekend;
- aanpassen van toegangsrechten van gebruikers van wie de rollen of functies zijn gewijzigd en toegangsrechten van gebruikers die de organisatie hebben verlaten onmiddellijk verwijderen of blokkeren;

Privacy

Ongeautoriseerde toegang vormt een bedreiging voor de privacy van betrokkenen. Een goed functionerend proces voor het toewijzen en intrekken van toegangsrechten is daarom cruciaal.

Bewijsvoering

Gebruikers krijgen bij de aanmaak van hun account toegang tot een aantal standaardomgevingen zoals de persoonlijke e-mail box. Voor toegang tot specifieke onderdelen van het netwerk of applicaties is een aanvraagprocedure / proces ingericht met goedkeuring van de proces-/systeemeigenaar. Deze ziet toe op (en is eindverantwoordelijk) voor het toekennen van de juiste autorisaties.

2 Overleg het vastgestelde beleid voor autorisatie- en authenticatie, bijvoorbeeld het IBP-beleid of een afzonderlijke richtlijn, waar de procedure voor het toekennen van toegangsrechten onderdeel van is.

3 Overleg een document waaruit blijkt dat de procedure voor toegang verlenen voor de kernsystemen (SIS/HR/FIN) formeel is geregeld en wordt daadwerkelijk wordt gevolgd.

Document	Handreiking autorisatie IBP in het mbo (IBPDOC37)
Zie ook	5.1, 5.2, 5.3, 5.5

Toetsingskader informatiebeveiliging				
Cluster	**5**	**Toegangsbeveiliging en integriteit**	**P**	AVG art. 5, 32
Statement	**5.5**	**Beheren van speciale toegangsrechten**		ISO 9.2.3

Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.

Toelichting
Denk bij speciale toegangsrechten bijvoorbeeld aan toegang tot operating systemen, databases en beheeraccounts van applicaties. Omdat een dergelijk account gebruik kan maken van een grote hoeveelheid privileges moet het gebruik van dergelijke beheerdersaccounts aan strikte regels en voorwaarden worden gekoppeld en tot een minimum worden beperkt.

Privacy
Als accounts met speciale toegangsrechten worden misbruikt, door de gebruiker van het account, of iemand die onbevoegd toegang heeft verkregen, dan kan dit grote gevolgen hebben voor de privacy van betrokkenen.

Bewijsvoering
Het toekennen van speciale toegangsrechten aan (systeem)beheerders is aantoonbaar aan strikte regels/voorwaarden gebonden en wordt actueel bijgehouden.

2 Overleg het vastgestelde beleid voor autorisatie- en authenticatie, bijvoorbeeld het IBP-beleid of een afzonderlijke richtlijn, waarin de uitgangspunten voor het toewijzen van speciale toegangsrechten zijn beschreven.

3 Overleg een lijst met de namen van de medewerkers met speciale toegangsrechten, inclusief onderbouwing waarom deze medewerkers deze speciale rechten hebben toegewezen gekregen.

Document	Handreiking autorisatie IBP in het mbo (IBPDOC37)
Zie ook	5.1, 5.2, 5.3, 5.4

Toetsingskader informatiebeveiliging				
Cluster	**5**	**Toegangsbeveiliging en integriteit**	**P**	AVG art. 5, 32
Statement	**5.6**	**Beheer van geheime authenticatie-informatie van gebruikers**		ISO 9.2.4

Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.

Toelichting
Het gaat hier om wachtwoordbeheer. Voor het verlenen van de toegang tot netwerken en systemen wordt veelal gebruikgemaakt van gebruikersnamen en wachtwoorden. Dit betekent dat wachtwoorden een belangrijk aspect vormen van de informatiebeveiliging en moeten worden beheerst via een formeel beheersproces.
Dit proces gaat onder andere in op:
- de verplichting om het wachtwoord geheim te houden en hierover een verklaring te ondertekenen;
- het verplicht wijzigen van het wachtwoord bij eerste gebruik;
- eisen ten aanzien van lengte, complexiteit en geldigheidsduur van het wachtwoord;

Privacy
Als een kwaadwillende gebruiker onbevoegd toegang krijgt door het compromitteren van een gebruikersaccount dan kan dit grote gevolgen hebben voor de privacy van betrokkenen.

Bewijsvoering
Er zijn goede procedures rond het beheer/gebruik van wachtwoorden en eventueel andere vormen van authenticatie.

2 Overleg het vastgestelde beleid voor autorisatie- en authenticatie, bijvoorbeeld het IBP-beleid of een afzonderlijke richtlijn, waarin het toewijzen van wachtwoorden en mogelijk andere vormen van geheime authenticatie-informatie zijn beschreven.

3 Overleg procesbeschrijvingen/werkinstructies rondom het wachtwoordbeheer, waarin duidelijk wordt aangetoond dat het toekennen/gebruiken van wachtwoorden is geregeld via een formeel beheersproces.

Document	Handreiking autorisatie IBP in het mbo (IBPDOC37)

Toetsingskader informatiebeveiliging				
Cluster	**5**	**Toegangsbeveiliging en integriteit**	**P**	AVG art. 32
Statement	**5.7**	**Geheime authenticatie-informatie gebruiken**		ISO 9.3.1

Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.

Toelichting
Het gaat hier om het gebruiken van wachtwoorden. Gebruikers moeten instructies krijgen voor de omgang met hun wachtwoord, bijvoorbeeld om het strikt geheim te houden, het niet te noteren en het onmiddellijk te wijzigen als er een vermoeden van misbruik bestaat. Ook moet de gebruiker een wachtwoord kiezen dat niet eenvoudig te raden is. De organisatie kan eisen stellen aan de minimale lengte en complexiteit van het wachtwoord.

Privacy
Als een kwaadwillende gebruiker onbevoegd toegang krijgt door het compromitteren van een gebruikersaccount dan kan dit grote gevolgen hebben voor de privacy van betrokkenen.

Bewijsvoering
Er zijn goede werkinstructies gericht op de eindgebruikers, in lijn met het vastgestelde beleid voor autorisatie- en authenticatie, voor het verantwoord gebruiken van wachtwoorden en eventueel andere vormen van authenticatie.

2 Overleg een werkinstructie waarin gebruikers uitleg krijgen over de eisen ten aanzien van wachtwoorden en mogelijk andere vormen van geheime authenticatie-informatie.

3 Overleg een document (bijvoorbeeld een printscreen) waaruit blijkt dat de werkinstructie m.b.t. het gebruik van wachtwoorden is gecommuniceerd.

Document	Handreiking autorisatie IBP in het mbo (IBPDOC37)
Zie ook	5.8, 5.9, 5.18

Toetsingskader informatiebeveiliging				
Cluster	**5**	**Toegangsbeveiliging en integriteit**	**P**	AVG art. 32
Statement	**5.8**	**Beperking toegang tot informatie**		ISO 9.4.1

Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.

Toelichting
Dit betekent dat de toegang tot een systeem fijnmazig moet zijn ingeregeld, door bijvoorbeeld onderscheid te maken in lees- en schrijfrechten, of door een deel van de gegevens af te schermen. Een en ander op basis van de autorisatie van de betreffende gebruiker, rekening houdend met de principes 'need to know' en 'least privilege'. Privacy by design is hier het sleutelwoord.

Privacy
De principes van de AVG schrijven voor dat er niet meer informatie mag worden gedeeld dan strikt noodzakelijk voor het uitvoeren van de werkzaamheden.

Bewijsvoering
Voor het beschermen van gegevens in systemen en toepassingen zijn toegangsbeperkingen ingericht op basis van "need-to-know" en/of "need-to-use". Het beveiligingsniveau wordt aangepast aan de gevoeligheid van de gegevens en systemen. Dit gebeurt op basis van de dataclassificatie.

2 Overleg een document (bijvoorbeeld een autorisatiematrix) waaruit blijkt dat voor tenminste de kernsystemen SIS en HR, de toegang tot bepaalde delen van informatie wordt beperkt tot specifieke rollen.

3 Op basis van een interview of waarneming ter plaatse wordt de werking van het document getoetst door de auditor. Een kort verslag wordt toegevoegd.

Document	Handreiking autorisatie IBP in het mbo (IBPDOC37)
Zie ook	5.7, 5.9, 5.18

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**5**	**Toegangsbeveiliging en integriteit**	**P**	**E**	AVG art. 5, 32
Statement	**5.9**	**Beveiligde inlogprocedures**			ISO 9.4.2

Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.

Toelichting
Om de identiteit van een gebruiker te bewijzen moet een passende authenticatietechniek worden gekozen. Vaak gaat het hier om wachtwoorden, maar op basis van de classificatie van het systeem/de gegevens kan een aanvullende of andere authenticatiemethode worden gebruikt, zoals cryptografische middelen, chipkaarten, tokens of biometrische middelen. Een goede inlogprocedure behoort onder meer:
- wachtwoorden niet weer te geven en versleuteld te versturen;
- zo min mogelijk informatie over het systeem of de toepassing openbaar te maken (bijv. niet aangeven welk deel van de login-informatie niet correct was);
- bestand te zijn tegen brute-force aanvallen;
- niet-succesvolle en succesvolle pogingen te registreren;
- inactieve sessies na een bepaalde time-out te beëindigen.

Privacy / Examinering
Als een kwaadwillende gebruiker onbevoegd toegang krijgt door het compromitteren van een gebruikersaccount dan kan dit grote gevolgen hebben voor de privacy van betrokkenen en/of de vertrouwelijkheid van examens.

Bewijsvoering
Alle netwerken en systemen van de onderwijsinstelling zijn slechts toegankelijk via een beveiligde inlogprocedure, volgens bovengenoemde uitgangspunten. Als de classificatie van de gegevens dat vereist wordt gebruikgemaakt van aanvullende authenticatie (MFA).

2 Overleg een door het CvB goedgekeurde versie van het IBP-beleid waar autorisatie- en authenticatiebeleid onderdeel van is.

3 Op basis van een interview of waarneming ter plaatse wordt de werking van het document getoetst door de auditor. Een kort verslag wordt toegevoegd.

Document	Handreiking autorisatie IBP in het mbo (IBPDOC37)
Zie ook	5.7, 5.8, 5.18

Toetsingskader informatiebeveiliging				
Cluster	**5**	**Toegangsbeveiliging en integriteit**	**P**	AVG art. 32
Statement	**5.10**	**Sleutelbeheer**		ISO 10.1.2

Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.

Toelichting
Het gaat hierbij om cryptografische sleutels die onder meer worden gebruikt voor het versleutelen van opslagmedia van laptops en verwijderbare media (bijvoorbeeld Bitlocker) of beveiligingscertificaten voor websites of webservices. Het aanmaken, bewaren, archiveren, terugvinden, distribueren, terugtrekken en vernietigen van dergelijke cryptografische sleutels dient onderdeel te zijn van het informatiebeveiligingsbeleid. Cryptografische sleutels behoren te worden beschermd tegen diefstal, onbevoegd gebruik, openbaarmaking en verlies. Concrete uitwerking van dit beleid kan zijn dat medewerkers worden verplicht om gebruik te maken van de door de organisatie aangeboden methoden van encryptie.

Privacy
Door gebruik te maken van versleuteling van gegevens worden zowel de kans als de impact van een incident waarbij persoonsgegevens worden gelekt beperkt.

Bewijsvoering
Het IBP-beleid bevat een richtlijn met betrekking tot "Cryptografische beheersmaatregelen".

2 Overleg een richtlijn "Cryptografische beheersmaatregelen".

3 Overleg een document waarin alle medewerkers in kennis worden gesteld van de richtlijn "Cryptografische beheersmaatregelen".

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**5**	**Toegangsbeveiliging en integriteit**	**P**	**E**	AVG art. 24, 32
Statement	**5.12**	**Beschermen van informatie in logbestanden**			ISO 12.4.2

Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.

Toelichting
Er moeten maatregelen genomen om informatie in logbestanden te beschermen tegen onbevoegde veranderingen en tegen operationele problemen met de logvoorziening, zoals:
- veranderingen aan de soorten berichten die worden vastgelegd;
- bewerken of verwijderen van logbestanden;
- overschrijden van de opslagcapaciteit van de media met de logbestanden, waardoor gebeurtenissen niet meer kunnen worden vastgelegd of eerder vastgelegde gebeurtenissen worden overschreven.

(Het gaat hier over de bescherming van de logbestanden, de logging zelf is geregeld in cluster 6; statement 6.2)

Privacy / Examinering
In het geval van een datalek of een beveiligingsincident m.b.t. examinering is het belangrijk dat er logbestanden aanwezig zijn om de oorzaak, achtergronden en impact van het incident te kunnen onderzoeken en daarover verantwoording af te kunnen leggen.

Bewijsvoering
Gebeurtenissen met betrekking tot de kernsystemen (SIS/HR/FIN) worden gelogd en deze logbestanden worden adequaat beschermd.

2 Overleg een beleidsdocument waarin het beschermen van informatie in logbestanden is vastgelegd.

3 Op basis van waarneming ter plaatse wordt de werking van het document getoetst door de auditor. Een kort verslag wordt toegevoegd.

Document	Model beleidsplan informatiebeveiliging en privacy (IBPDOC6)
Zie ook	6.2

Toetsingskader informatiebeveiliging					
Cluster	**5**	**Toegangsbeveiliging en integriteit**			AVG art. 32
Statement	**5.14**	**Beveiliging van netwerkdiensten**			ISO 13.1.2
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.					
Toelichting Het gaat hierbij om diensten op het gebied van netwerkaansluitingen, beheerde netwerkdiensten, levering en beheer van firewalls. De waarborgen van de leverancier om de overeengekomen diensten veilig te beheren moeten contractueel worden vastgesteld waarbij ook het recht om dit te controleren, bijvoorbeeld in de vorm van een audit is geregeld. Ook kunnen er waarborgen worden gevraagd en geboden ten aanzien van de certificering van de leverancier (bijv ISO 27001)					
Bewijsvoering Met leveranciers van netwerkdiensten zijn goede contractuele afspraken gemaakt met betrekking tot de beveiliging van netwerkdiensten.					
2 Overleg een beleidsdocument aangaande de beveiliging van netwerkdiensten, bestaande uit contracten, SLA's, SLR's etc.					
3 Op basis van waarneming ter plaatse wordt de werking van het document getoetst door de auditor. Een kort verslag wordt toegevoegd.					
Zie ook	Wetsvoorstel Digitale Overheid (WDO) Uniforme Beveiligingsvoorschriften				

Toetsingskader informatiebeveiliging					
Cluster	**5**	**Toegangsbeveiliging en integriteit**			AVG art. 32
Statement	**5.15**	**Scheiding in netwerken**			ISO 13.1.3
Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.					
Toelichting Een van de methoden om de beveiliging van grote netwerken te beheren is ze te verdelen in gescheiden netwerkdomeinen, bijvoorbeeld door een administratief netwerk af te scheiden van een studentennetwerk. De scheiding kan tot stand worden gebracht door fysiek verschillende netwerken, of door verschillende logische netwerken te gebruiken.					
Bewijsvoering Het netwerk is opgedeeld in VLAN's, zoals: personeel, studenten, examinering, telefoon, multifunctionals, camera's, gasten, etc.					
2	Overleg een document waarin aangegeven wordt dat de onderwijsinstelling gebruikt maakt van VLAN's				
3	Op basis van waarneming ter plaatse wordt de werking van het document getoetst door de auditor. Een kort verslag wordt toegevoegd.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**5**	**Toegangsbeveiliging en integriteit**	**P**	**E**	AVG art. 32
Statement	**5.16**	**Elektronische berichten**			ISO 13.2.3

Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.

Toelichting
Denk daarbij aan:
- berichten beschermen tegen onbevoegde toegang of wijziging, rekening houdend met de classificatie van de berichten;
- correcte adressering en transport van het bericht waarborgen;
- wettelijke eisen, bijvoorbeeld voor elektronische handtekeningen.

Privacy / Examinering
Als gevoelige informatie wordt verstuurd via (bijvoorbeeld) e-mail dan moeten deze berichten beschermd worden tegen onbevoegde toegang.

Bewijsvoering
Berichten die gevoelige informatie bevatten worden passend beschermd, bijvoorbeeld door gebruik te maken van een beveiligde e-mailtoepassing of bestandsoverdracht via een toepassing als 'SURF Filesender'.

2 Overleg een document/richtlijn/werkinstructie waarin wordt aangegeven dat berichten met gevoelige informatie op een beveiligde manier verstuurd dienen te worden.

3 Op basis van waarneming ter plaatse wordt de werking van het document getoetst door de auditor. Een kort verslag wordt toegevoegd.

Document	
Zie ook	Wetsvoorstel Digitale Overheid (WDO) Uniforme Beveiligingsvoorschriften Veilige e-mail coalitie

Toetsingskader informatiebeveiliging					
Cluster	**5**	**Toegangsbeveiliging en integriteit**			AVG art. 24
Statement	**5.17**	**Transacties van toepassingen beschermen**			ISO 14.1.3

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.

Toelichting
Voorbeelden van transacties binnen de onderwijspraktijk zijn het digitaal aanmelden, inschrijven, uitschrijven enzovoort. Hierbij wordt met veel partijen uitgewisseld (koppelpunt mbo, gemeenten, DUO etc.)
Belangrijke aandachtspunten hierbij:
- het gebruik van elektronische handtekeningen door alle partijen die bij de transactie betrokken zijn;
- bewaking dat alle aspecten van de transactie worden afgehandeld;
- versleuteling van de communicatiepaden tussen alle betrokken partijen;
- beveiliging van protocollen die worden gebruikt om te communiceren tussen alle betrokken partijen;
- veilige opslaglocatie van transactiegegevens en logbestanden.

Bewijsvoering
Belangrijke transacties, zoals digitaal aanmelden, inschrijven en uitschrijven zijn aantoonbaar goed geregeld, koppelvlakken met externe partijen, uitwisselingsprotocollen en dergelijke zijn actueel in beeld. Voor bedrijfskritische processen wordt een DPIA uitgevoerd.

2 Overleg een document waarin de belangrijkste transacties zijn beschreven, inclusief applicatielandschap, koppelvlakken en beveiligingscertificaten.

3 Op basis van waarneming ter plaatse wordt de werking van het document getoetst door de auditor. Een kort verslag wordt toegevoegd.

Zie ook	Wetsvoorstel Digitale Overheid (WDO) Uniforme Beveiligingsvoorschriften

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**5**	**Toegangsbeveiliging en integriteit**			AVG art. 32
Statement	**5.18**	**Systeem voor wachtwoordbeheer**			ISO 9.4.3

Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.

Toelichting

Een systeem voor wachtwoordbeheer behoort onder meer:

- het gebruik van unieke accounts af te dwingen om de toerekenbaarheid te handhaven;
- gebruikers de mogelijkheid te bieden hun eigen wachtwoord te kiezen en te wijzigen, en een bevestigingsprocedure te bevatten die rekening houdt met foutieve invoer;
- de keuze voor sterke wachtwoorden af te dwingen;
- gebruikers te dwingen hun wachtwoord bij het eerste inloggen te wijzigen;
- een registratie van eerder gebruikte wachtwoorden bij te houden en te voorkomen dat deze opnieuw worden gebruikt;
- wachtwoorden in beschermde vorm op te slaan en te versturen.

Bewijsvoering

De systemen waarin wachtwoorden worden beheerd voldoen aan het vastgestelde beleid voor autorisatie- en authenticatie en voorzien tenminste in de bovengenoemde uitgangspunten.

2 Overleg het vastgestelde beleid voor autorisatie- en authenticatie, bijvoorbeeld het IBP-beleid of een afzonderlijke richtlijn, waarin de eisen met betrekking tot het gebruik van wachtwoorden zijn beschreven.

3 Op basis van waarneming ter plaatse wordt de werking van het document getoetst door de auditor. Een kort verslag wordt toegevoegd. Eventueel kan de werking worden aangetoond door middel van bijvoorbeeld printscreens waaruit blijkt dat er foutmeldingen komen als de gebruiker niet voldoet aan het vastgestelde beleid.

Document	Handreiking autorisatie IBP in het mbo (IBPDOC37)
Zie ook	5.7, 5.8, 5.9

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**5**	**Toegangsbeveiliging en integriteit**			AVG art. 32
Statement	**5.19**	**Speciale systeemhulpmiddelen gebruiken**			ISO 9.4.4
Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.					
Toelichting De meeste computersystemen hebben een of meer systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen. Denk bijvoorbeeld aan een tool voor het bekijken van records in databases waarbij de autorisatie van het systeem wordt gepasseerd. Het gebruik van dergelijke vormen van speciale systeemhulpmiddelen dient zo veel mogelijk te worden beperkt en alleen toegankelijk te zijn voor specifieke beheerders. Bovendien moet het gebruik worden gelogd.					
Bewijsvoering Het gebruik van dergelijke speciale systeemhulpmiddelen is aantoonbaar aan duidelijke regels gebonden.					
2	Overleg het beleid/de regeling met betrekking tot het gebruik van speciale systeemhulpmiddelen.				
3	Overleg een lijst met de namen/functies van de medewerkers die toegang hebben tot speciale systeemhulpmiddelen en controleer, bijvoorbeeld door een interview, of deze op de hoogte zijn van het beleid inzake speciale systeemhulpmiddelen en daar naar handelen.				
Document					

Toetsingskader informatiebeveiliging					
Cluster	**5**	**Toegangsbeveiliging en integriteit**			AVG art. 32
Statement	**5.23**	**Procedures voor wijzigingsbeheer met betrekking tot systemen**			ISO 14.2.2
Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.					
Toelichting Er dienen formele procedures voor wijzigingsbeheer te worden gevolgd om de integriteit van het systeem te waarborgen. Nieuwe systemen en belangrijke wijzigingen aan bestaande systemen volgen een formeel proces van documentatie, specificatie, testen, kwaliteitscontrole en beheerde implementatie. Dit proces behoort een risicobeoordeling, een analyse van de gevolgen van wijzigingen en een specificatie van de nodige beveiligingsbeheersmaatregelen te omvatten. Dit proces behoort ook te waarborgen dat bestaande beveiligings- en beheersingsprocedures niet worden gecompromitteerd.					
Bewijsvoering Binnen de organisatie is een goed functionerend proces van wijzigingenbeheer ingeregeld.					
2	Overleg een document waaruit blijkt dat het proces van wijzigingenbeheer is beschreven.				
3	Overleg een lijst/rapport/printscreen met recente wijzigingen waaruit duidelijk blijkt dat het wijzigingenbeheer volgens een formeel proces (zie toelichting) wordt uitgevoerd.				
Zie ook	4.1				

Toetsingskader informatiebeveiliging				
Cluster	**5**	**Toegangsbeveiliging en integriteit**	**P**	AVG art. 32
Statement	**5.27**	**Bescherming van testgegevens**		ISO 14.3.1

Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.

Toelichting
Systeem- en acceptatietests vereisen vaak grote hoeveelheden testgegevens die een zo getrouw mogelijke weergave moeten zijn van operationele gegevens. Het voor testdoeleinden gebruiken van operationele databases met persoonsgegevens of enige andere vertrouwelijke informatie behoort daarbij te worden vermeden. Indien persoonsgegevens of anderszins vertrouwelijke informatie wordt gebruikt voor testdoeleinden, behoren alle gevoelige details en inhoud te worden beschermd door deze te verwijderen of te wijzigen.

Privacy
Bij het testen van systemen waarbinnen persoonsgegevens worden verwerkt moet extra aandacht zijn voor het beschermen van deze gegevens.

Bewijsvoering
Bij het testen van systemen wordt gebruikgemaakt van (geanonimiseerde) testgegevens en/of een beveiligde acceptatie-omgeving.

2 Overleg een document/richtlijn waaruit blijkt dat er bij het testen van systemen speciale aandacht is voor de bescherming van persoonsgegevens of andere vertrouwelijke informatie. Voor SaaS dienen deze eisen te zijn opgenomen in de leverancierscontracten.

3 Op basis van een interview of waarneming ter plaatse wordt de werking van het document getoetst door de auditor. Een kort verslag wordt toegevoegd.

Document	

6. Controle en logging

Nr.	ISO27002	Statement
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers
6.2	12.4.1	Gebeurtenissen registreren
6.3	12.4.3	Logbestanden van beheerders en operators
6.4	*vervallen*	
6.5	*vervallen*	
6.6	14.2.9	Systeemacceptatietests
6.7	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers
6.8	16.1.7	Verzamelen van bewijsmateriaal
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen
6.10	18.2.3	Beoordeling van technische naleving
6.11	*vervallen*	
6.12	12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen
6.13	16.1.6	Lering uit informatiebeveiligingsincidenten
6.14	18.2.1	Onafhankelijke beoordeling van informatiebeveiliging

Terug naar index clusters

Toetsingskader informatiebeveiliging					
Cluster	**6**	**Controle en logging**	**P**	**E**	AVG art.32
Statement	**6.1**	**Beoordeling van toegangsrechten van gebruikers**			ISO 9.2.5

Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.

Toelichting
Het management behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces:

- toegangsrechten van gebruikers behoren regelmatig en na wijziging of beëindiging van het dienstverband te worden beoordeeld en zo nodig te worden aangepast;
- autorisaties voor speciale toegangsrechten behoren vaker te worden beoordeeld;
- van wijzigingen in speciale accounts behoren voor periodieke beoordeling logbestanden te worden bijgehouden.

Privacy / Examinering
Het correct toekennen van autorisaties is een belangrijke voorwaarde voor goede bescherming van vertrouwelijke gegevens, zeker als het gaat om speciale toegangsrechten.

Bewijsvoering
De toegangsrechten, ook tijdelijke toegangsrechten, worden door het management toegekend aan de medewerkers die zij formeel aansturen.
Controle hierop zal in de praktijk vaak inhouden dat de applicatiebeheerder een overzicht genereert van alle personen die toegang hebben tot de applicatie, met de bijbehorende rechten. De eindverantwoordelijke (systeemeigenaar of proceseigenaar, meestal een directeur of hoofd) controleert dit overzicht en geeft aan wat eventueel gewijzigd moet worden. Dit resultaat wordt vastgelegd. Deze beoordelingsprocedure moet geregeld gebeuren (aantal keren per jaar).

2 Overleg een vastgesteld overzicht toegangsrechten op basis van de autorisatiematrix. Dit is de gewenste vastgestelde situatie (SOLL).

3 Overleg recente overzichten van toegangsrechten voor de kernapplicaties (SIS/HR/FIN), geaccordeerd de eindverantwoordelijke (systeem- of proceseigenaar).

Document	Handreiking autorisatie IBP in het mbo (IBPDOC37)
Zie ook	2.3, 5.3

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**6**	**Controle en logging**	**P**	**E**	AVG art.32
Statement	**6.2**	**Gebeurtenissen registreren**			ISO 12.4.1

Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

Toelichting
Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.
Logbestanden behoren onder meer de volgende gegevens te bevatten:
- gebruikers-ID's;
- data, tijdstippen en details van in- en uitloggen;
- identiteit device/locatie;
- netwerkadressen en -protocollen;
- geslaagde/geweigerde pogingen om toegang te krijgen;
- gebruik van speciale bevoegdheden en dergelijke.

Gebruikers moeten worden geïnformeerd dat dergelijke activiteiten worden gelogd. De logbestanden kunnen gevoelige en persoonsgegevens bevatten en moeten daarom goed worden beschermd.

Systeembeheerders mogen logbestanden van hun eigen activiteiten niet bewerken, wissen of deactiveren (zie ook 6.3)

Privacy / Examinering
Goede logbestanden zijn een voorwaarde om onderzoek te kunnen doen naar de aanleiding, achtergronden en de impact van informatiebeveiligingsgebeurtenissen zoals datalekken en fraude bij examinering.

Bewijsvoering
Logbestanden met activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen zijn beschikbaar en kunnen worden geraadpleegd, bijvoorbeeld als er sprake is van incidenten.

2 Overleg een overzicht van categorieën van gegevens die worden gelogd binnen tenminste de kernsystemen (SIS/HR/FIN), voor zover de applicatie deze logging redelijkerwijs ondersteunt.

3 Overleg een overzicht van logbestanden van tenminste de kernsystemen (SIS/HR/FIN), waaruit blijkt dat gebruikersactiviteiten van medewerkers, inclusief tijdelijke medewerkers, daadwerkelijk zijn gelogd en voor beheerders toegankelijk zijn om te worden beoordeeld.

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**6**	**Controle en logging**		E	AVG art.32
Statement	**6.3**	**Logbestanden van beheerders en operators**			ISO 12.4.3

Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.

Toelichting
Houders van een speciaal account (bijvoorbeeld systeembeheerders) zijn mogelijk in staat om de logbestanden die onder hun directe beheer staan te manipuleren. Daarom is het nodig de logbestanden hiervoor te beschermen en te hierop te controleren.

Examinering
Om eventuele examenfraude door interne medewerkers op te kunnen sporen/uit te kunnen sluiten is het belangrijk dat medewerkers met speciale rechten de logbestanden niet onopgemerkt kunnen aanpassen.

Bewijsvoering
Logbestanden met activiteiten van beheerders van het netwerk zijn beschikbaar en kunnen worden geraadpleegd, bijvoorbeeld als er sprake is van incidenten. Deze logbestanden zijn beschermd tegen manipulatie door beheerders, bijvoorbeeld door back-up, remote opslag, hashing/fingerprinting.

2 Overleg een document waaruit blijkt dat beheeractiviteiten van systeembeheerders worden gelogd.

3 Overleg een rapport waaruit blijkt dat deze logbestanden daadwerkelijk worden gecontroleerd door leidinggevende. Als alternatief kan op basis van een interview of waarneming ter plaatse de werking van het document worden getoetst door de auditor. Een kort verslag wordt toegevoegd.

Toetsingskader informatiebeveiliging					
Cluster	**6**	**Controle en logging**			AVG art. 24
Statement	**6.6**	**Systeemacceptatietests**			ISO 14.2.9

Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.

Toelichting
Er zijn aanvaardingscriteria vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er wordt een geschikte acceptatietest van het systeem of de systemen uitgevoerd alvorens deze worden overgezet naar de productieomgeving.

Bewijsvoering
Bij de invoer van nieuwe informatiesystemen, of bij belangrijke updates van bestaande systemen worden acceptatietest ontwikkeld en uitgevoerd.

2 Overleg een document waaruit blijkt dat er een procedure en aanvaardingscriteria zijn opgesteld voor systeemacceptatietesten van tenminste de kernapplicaties (SIS/HR/FIN).

3 Overleg documenten waaruit blijkt dat nieuwe (versies van) kernapplicaties formeel getest zijn door de gebruikersorganisatie op basis van een checklist/acceptatieformulier.

Toetsingskader informatiebeveiliging					
Cluster	**6**	**Controle en logging**			AVG art. 28
Statement	**6.7**	**Monitoring en beoordeling van dienstverlening van leveranciers**			ISO 15.2.1

Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.

Toelichting
Het monitoren en beoordelen van dienstverlening van leveranciers is belangrijk om te waarborgen dat aan de voorwaarden van informatiebeveiliging wordt voldaan en dat incidenten en problemen op het gebied van informatiebeveiliging op de juiste manier worden behandeld. In verband daarmee kan de organisatie de prestatieniveaus van de dienstverlening monitoren om naleving van de overeenkomsten te controleren. Verder kan de organisatie audits van leveranciers of pentests op de systemen (laten) uitvoeren.

Bewijsvoering
Verwerkersovereenkomsten en SLA's worden periodiek gecontroleerd op naleving door de leveranciers.

2 Overleg een document waaruit blijkt dat er een procedure is opgesteld voor de periodieke beoordeling van de dienstverlening van leveranciers.

3 Overleg documenten waaruit blijkt dat leveranciers en/of hun systemen recent zijn beoordeeld, bijvoorbeeld aan de hand van een supplier scorecards, auditrapporten of pentests.

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**6**	**Controle en logging**			AVG art. 33
Statement	**6.8**	**Verzamelen van bewijsmateriaal**			ISO 16.1.7

De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.

Toelichting
Als na een informatiebeveiligingsincident juridische maatregelen moeten worden genomen (civiel of strafrechtelijk), moet geldig bewijsmateriaal worden verzameld, bewaard en gepresenteerd. Daarbij moet o.a. rekening gehouden worden met:
- de toelaatbaarheid van het bewijs in een rechtszaak;
- de kwaliteit en volledigheid van het bewijsmateriaal;
- beheersmaatregelen die zijn genomen om het verkregen bewijsmateriaal te beschermen.

Forensisch onderzoek dient te worden uitgevoerd door externe deskundigen.

Bewijsvoering
Forensisch onderzoek naar aanleiding van informatiebeveiligingsincidenten wordt uitgevoerd door externe hierin gespecialiseerde partijen of er zijn afspraken gemaakt met dergelijke externe partijen, mocht dat nodig zijn in de opvolging/opsporing van informatiebeveiligingsincidenten.

2 Overleg een document waaruit blijkt dat er voor forensisch onderzoek een extern deskundig bedrijf (bijvoorbeeld Fox IT, Hoffman, etc.) wordt ingeschakeld.

3 Overleg een document waaruit blijkt, dat forensisch onderzoek door een externe partij is uitgevoerd.

Toetsingskader informatiebeveiliging				
Cluster	**6**	**Controle en logging**	**P**	AVG art. 24
Statement	**6.9**	**Naleving van beveiligingsbeleid en -normen**		ISO 18.2.2

De directie 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.

Toelichting
Managers dienen te beoordelen of wordt voldaan aan informatiebeveiligingseisen zoals gedefinieerd in beleidsregels, normen en andere toepasselijke regelgeving en zo nodig passende corrigerende maatregelen te implementeren.

Privacy
Voor een goede bescherming van de privacy is de controle op naleving cruciaal en dit dient daarom belegd te zijn op managementniveau.

Bewijsvoering
Er wordt regelmatig (minimaal 1x per jaar) getoetst of het IBP-beleid wordt nagekomen.

2 Overleg een document waaruit blijkt dat er minimaal jaarlijks wordt gecontroleerd op naleving van het IBP-beleid, bijvoorbeeld d.m.v. een auditplan of deelname aan IBP-benchmarks.

3 Overleg een document waaruit blijkt dat deze audits daadwerkelijk zijn uitgevoerd en hebben geleid tot concrete verbetermaatregelen.

Toetsingskader informatiebeveiliging				
Cluster	**6**	**Controle en logging**	**P**	AVG art. 32
Statement	**6.10**	**Beoordeling van technische naleving**		ISO 18.2.2

Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.

Toelichting
Beoordelingen van technische naleving omvatten onderzoek van productiesystemen om te waarborgen dat beheersmaatregelen voor hardware en software correct zijn geïmplementeerd. Dit soort beoordeling van naleving vereist specialistische technische expertise. Het gaat hierbij om penetratietests en andere vormen kwetsbaarheidsbeoordelingen.

Privacy
Voor een goede bescherming van de privacy moet de beveiliging van de informatiesystemen op orde zijn en regelmatig worden beoordeeld.

Bewijsvoering
De beveiliging van het netwerk en de applicaties wordt regelmatig door een onafhankelijke derde getest.

2 Overleg een document waaruit blijkt dat er regelmatig een externe test wordt uitgevoerd ter beoordeling van de technische beveiliging.

3 Overleg een document waaruit blijkt dat dergelijke tests (bijvoorbeeld een pen-test) daadwerkelijk zijn uitgevoerd en hebben geleid tot concrete verbetermaatregelen.

Toetsingskader informatiebeveiliging					
Cluster	**6**	**Controle en logging**			AVG art. 32
Statement	**6.12**	**Beheersmaatregelen betreffende audits van informatiesystemen**			ISO 16.1.7

Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.

Toelichting

Het gaat hier om de planning en uitvoering van audits op de informatiesystemen en netwerken, bijvoorbeeld een pentest. Dergelijke tests kunnen schadelijk zijn wanneer ze niet goed doordacht worden ingezet. Belangrijke aandachtspunten daarbij:

- audittests behoren te worden beperkt tot alleen-lezen-toegang tot software en gegevens;
- als de test ook toegang anders dan 'alleen lezen' verlangt, dan mag deze alleen worden uitgevoerd op geïsoleerde kopieën van bestanden;
- audittests die de beschikbaarheid van systemen kunnen beïnvloeden, behoren buiten werkuren plaats te vinden;
- alle toegangshandelingen behoren te worden gemonitord en vastgelegd in een logbestand.

Bewijsvoering

Pentests en vergelijkbare audittest worden zodanig gepland en uitgevoerd dat de bedrijfsvoering niet wordt verstoord en er geen schade of nieuwe kwetsbaarheden door ontstaan.

2 Overleg een document waaruit blijkt dat er strikte randvoorwaarden gelden voor het plannen en uitvoeren van audittests, zoals een pentest.

3 Overleg een document waaruit blijkt dat bij de uitvoering van een dergelijke test rekening is gehouden deze randvoorwaarden.

Toetsingskader informatiebeveiliging					REGIEGROEP IBP IN HET MBO Kennisnet SURF saMBO-ICT
Cluster	**6**	**Controle en logging**			AVG art. 33
Statement	**6.13**	**Lering uit informatiebeveiligingsincidenten**			ISO 16.1.6

Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.

Toelichting
Informatiebeveiligingsincidenten moeten worden geregistreerd, inclusief de technische, procesmatige of menselijk oorzaak, de omvang, de kosten en andere achtergrondinformatie. Incidenten dienen te worden geëvalueerd en daaruit kan de noodzaak blijken van uitgebreidere of aanvullende beheersmaatregelen. Op die manier kan herhaling van een dergelijk incident in de toekomst worden voorkomen.

Bewijsvoering
Informatiebeveiligingsincidenten worden geregistreerd, inclusief de technische, procesmatige of menselijk oorzaken en deze informatie wordt gebruikt om vergelijkbare incidenten in de toekomst te voorkomen.

2 Overleg een document, bijvoorbeeld een verbeterregister of een rapportage uit Topdesk, waaruit blijkt dat incidenten worden geëvalueerd.

3 Overleg een document, bijvoorbeeld een jaarplan IBP, waaruit blijkt dat de in het verbeterregister gesignaleerd kwetsbaarheden vertaald zijn naar concrete maatregelen.

Toetsingskader informatiebeveiliging					
Cluster	**6**	**Controle en logging**			AVG art. 24
Statement	**6.14**	**Onafhankelijke beoordeling van informatiebeveiliging**			ISO 18.2.1

De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.

Toelichting
Het College van Bestuur moet jaarlijks een onafhankelijke beoordeling van het Informatiebeveiligings- en privacybeleid laten uitvoeren door een onafhankelijke functionaris. Dit kan zijn een onafhankelijke functionaris binnen de organisatie of een externe deskundige. Deze functionaris geeft een oordeel over het uitgevoerde self-assessment (de uitkomsten van dit toetsingskader) in een rapport van bevindingen (de aangegeven volwassenheidsniveaus kloppen) en eventueel aanbevelingen om gesignaleerde knelpunten op te lossen.

Bewijsvoering
De ingevulde Benchmark IBP wordt door een onafhankelijke derde gereviewd. Daarbij wordt de door de organisatie gescoorde volwassenheid vastgesteld, vaak op basis van een steekproef. Deze review vindt bij voorkeur plaats in het kader van de mbo-brede 'Peer Review', door een collega IBP-manager van een andere mbo-instelling.

2 Overleg een rapport van bevindingen op basis van een interne audit of peer review.

3 Overleg een document waaruit blijkt dat de bevindingen zijn gerapporteerd en/of vastgelegd, bijvoorbeeld in een verbeterregister of IBP-jaarplan.

Zie ook	6.9