Bijlage VIII.a Passende technische en organisatorische maatregelen

De AVG verplicht de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen die waarborgen dat de gegevens adequaat zijn beveiligd en gegevens beschermd zijn tegen ongeoorloofde verwerking en tegen verlies, vernietiging of beschadiging.

Normenkader informatiebeveiliging in het onderwijs

Kennisnet heeft de risico's in kaart gebracht die een rol spelen bij informatiebeveiliging binnen onderwijsinstellingen.[1] Deze risico's zijn vervolgens gekoppeld aan NEN- en ISO normen (het uitgangspunt als het gaat om de beveiliging van (persoons)gegevens) en door Kennisnet, SURF en saMBO-ICT voor het middelbaar beroepsonderwijs (mbo) vertaald in een 'normenkader'.[2]

Door de maatregelen uit dit normenkader na te leven is de onderwijsinstelling verzekerd dat zij haar persoonsgegevens adequaat heeft beveiligd. Dit normenkader is tevens bruikbaar voor het funderend onderwijs. Naar verwachting ontwikkelt Kennisnet op termijn ook voor het primair en voortgezet onderwijs een eigen variant.

Het mbo normenkader is onderscheiden in zes deelgebieden:

- het beleid met betrekking tot gegevensverwerkingen (organisatie);
- personeel, leerlingen en bezoekers;
- ruimtes en apparatuur;
- continuïteit;
- vertrouwelijkheid en integriteit;
- controle en logging.

De maatregelen die de onderwijsinstelling dient te nemen op basis van dit normenkader zijn door Kennisnet beschreven en (één-op-één) overgenomen in **bijlage VIII.b**.

Deze maatregelen dienen door de onderwijsinstelling te worden vertaald in beleid. Voor een deel kunt u hiervoor de modellen en protocollen (de bijlagen) bij het handboek gebruiken. Daarnaast zal op bestuursniveau uitvoering moeten worden gegeven aan (een deel van) de maatregelen en dient de onderwijsinstelling voor de maatregelen waar het handboek niet in voorziet aanvullend (en organisatie-specifiek) beleid te ontwikkelen.

In bijlage 1 is opgenomen welke modellen en protocollen bij het handboek kunnen worden gebruikt en welke maatregelen op bestuursniveau moeten worden uitgevoerd. Op de punten waar aanvullend beleid nodig is wordt waar mogelijk verwezen naar bruikbare documenten van Kennisnet en saMBO-ICT.

---

1 https://www.sambo-ict.nl/wp-content/uploads/2017/09/IBPDOC29-Handleiding-Risico-management-versie-1.2.docx, bijlage 1: Overzicht risico's en maatregelen ISO27002/2013

2 https://www.sambo-ict.nl/wp-content/uploads/2015/02/IBBDOC2-Normenkader-Informatiebeveiliging-MBO-versie-1.0-Creative-Commons.pdf en https://www.nen.nl/NEN-Shop/Norm/NENENISOIEC-270012017-en.htm.

Gegevensuitwisseling buiten de EU

Als persoonsgegevens worden doorgegeven aan een land buiten de Europese Economische Ruimte (EER) moet er sprake zijn van een beveiligingsniveau dat vergelijkbaar is met het beveiligingsniveau onder de AVG (zie ook de toelichting bij bijlage 3 van het Register). Om dit te waarborgen zijn er de volgende mogelijkheden:

a) doorgifte op basis van een adequaatheidsbesluit van de Europese Commissie;
b) doorgifte op basis van passende waarborgen, wanneer een land of organisatie niet als adequaat is aangemerkt door de Europese Commissie kan doorgifte plaatsvinden als de verwerkersverantwoordelijke en de verwerker (aantoonbaar) voorzien in passende waarborgen en afdwingbare rechten en rechtsmiddelen voor betrokkene(n);
c) doorgifte op basis van uitdrukkelijke toestemming van de betrokkene waarbij de betrokkene geïnformeerd is over de risico's, of wanneer sprake is van een situatie van noodzaak.

Gegevensuitwisseling naar de VS

De Europese Commissie (EC) heeft een regeling vastgesteld voor doorgifte van persoonsgegevens aan de Verenigde Staten (VS). Deze regeling heet het EU-VS privacy shield (privacyschild). Het doel van het privacy shield is bij uitwisseling van persoonsgegevens met de VS een beschermingsniveau te bieden dat in grote lijnen overeenkomt met het niveau binnen de Europese Unie (EU).

Het privacy shield komt in de plaats van de Safe Harbour-overeenkomst, die het Europees Hof van Justitie op 6 oktober 2015 ongeldig verklaarde. Elke organisatie in de VS die gecertificeerd is bij het privacy shield, heeft een passend beschermingsniveau (voor de duur van de certificatie). Dat betekent dat organisaties vanuit Europa persoonsgegevens mogen doorgeven naar deze organisaties in de VS.

Bijlage VIII.b Maatregelen voor informatiebeveiliging en bescherming van persoonsgegevens

Bron: IBPDOC2A Normenkader informatiebeveiliging MBO versie 2.0 zoals ontwikkeld door Kennisnet, SURF en saMBO-ICT

1. Beleid en organisatie

Maatregelen	Beleid
Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur.	Reglement met bijlagen (privacyhandboek)
Het door het bestuur vastgestelde Informatiebeveiligingsbeleid wordt gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Bijlage XIV, Bijlage XIII
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.	Auditbeleid (niet in het handboek opgenomen) Zie handboek saMBO-ICT: https://www.sambo-ict.nl/wp-content/uploads/2015/02/IBBDOC3-Handboek-MBOaudit-versie-1.1-Creative-Commons.pdf
Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Vaststellen op bestuursniveau.
Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	Door bestuurder te beleggen indien aan de orde.
Er dient beleid te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	Bijlage III, BYOD beleid (niet in het handboek opgenomen) Zie handreiking door saMBO-ICT en Kennisnet: www.sambo-ict.nl/wp-content/uploads/2013/06/HoeZo-Bring-Your-Own-Device.pdf
Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Bijlage I
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.	Bijlage I

Maatregelen	Beleid
Ter bescherming van informatie behoort een beleid voor het gebruik van crypto grafische beheersmaatregelen te worden ontwikkeld.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van crypto grafische beheersmaatregelen wordt geïmplementeerd.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	Bijlage III
Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	Bijlage III
Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Bijlage XI, Bijlage XII
De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Door de bestuurder te beleggen indien aan de orde.
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.	Bijlage XI, Bijlage XII
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.	Bijlage XI, Bijlage XII
Er zijn leidinggevende en -procedures vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Bijlage XIII Zie ook het dossier DDoS-aanval op school in de aanpak IBP van Kennisnet: https://maken.wikiwijs.nl/81891/Aanpak_IBP_voor_het_PO_en_VO#!page-3692866

Maatregelen	Beleid
Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	Bijlage XIII Zie ook het dossier DDoS-aanval op school in de aanpak IBP van Kennisnet: https://maken.wikiwijs.nl/81891/Aanpak_IBP_voor_het_PO_en_VO#!page-3692866
Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Reglement met bijlagen (privacyhandboek)
Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Reglement met bijlagen (privacyhandboek)
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.	Taak HR/bestuurder bij opstellen functiebouwwerk.

2. Personeel

Maatregelen	Beleid
De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	Bijlage V, Aanstellings- c.q. benoemingsbeleid (niet in het handboek opgenomen)
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.	Bijlage VI, Scholingsagenda (niet in het handboek opgenomen). Zie het stappenplan voor de implementatie bij het handboek en - de brochure ICT bekwaamheid door saMBO-ICT: https://www.kennisnet.nl/fileadmin/kennisnet/publicatie/hoezo/Hoe_Zo_Ict-bekwaamheid_in_het_mbo.pdf - het onderdeel bewustwording binnen de aanpak IBP door Kennisnet: https://maken.wikiwijs.nl/81891/Aanpak_IBP_voor_het_PO_en_VO#!page-2201401
De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	Bijlage I, Autorisatiebeleid (niet in het handboek opgenomen)
Er behoort een ‘clear desk’-beleid voor papieren documenten en verwijderbare opslagmedia en een ‘clear screen’-beleid voor informatie verwerkende faciliteiten te worden ingesteld.	Clear desk- en screenbeleid (niet in het handboek opgenomen)
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.	Periodieke audit naleving AVG
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.	Bijlage 1 bij bijlage III

Maatregelen	Beleid
Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.	Aanstellings- c.q. benoemingsbeleid (niet in het handboek opgenomen)

3. Ruimtes en apparatuur

Maatregelen	Beleid
Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.	Bijlage III, BYOD beleid (niet in het handboek opgenomen) Zie handreiking door saMBO-ICT en Kennisnet: www.sambo-ict.nl/wp-content/uploads/2013/06/HoeZo-Bring-Your-Own-Device.pdf
Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Taak ICT-verantwoordelijke
Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	Bijlage I, bijlage 2, toegangsrechten informatie
Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Bijlage I, bijlage 2, toegangsrechten informatie
Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	Taak door bestuurder te beleggen op locatieniveau
Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	Uitvoeren op bestuursniveau.
Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	Aanvulling op Bijlage I, bijlage 2 (niet in het handboek opgenomen)
Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.	Taak door bestuurder te beleggen op locatieniveau.
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.	Taak door bestuurder te beleggen op locatieniveau.

Maatregelen	Beleid
Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
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.	Bijlage III, BYOD beleid.
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.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)

4. Continuïteit

Maatregelen	Beleid
Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	Bijlage VI
Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten ten aanzien van het gevaar van virussen en dergelijke.	Bijlage VI, Scholingsagenda (niet in het handboek opgenomen). Zie het stappenplan voor de implementatie bij het handboek en de brochure ICT bekwaamheid door saMBO-ICT: https://www.kennisnet.nl/fileadmin/kennisnet/publicatie/hoezo/Hoe_Zo_Ict-bekwaamheid_in_het_mbo.pdf
Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt.	Back-up beleid (niet in het handboek opgenomen)
Gemaakte back ups worden regelmatig getest conform het back-up beleid.	Auditbeleid (niet in het handboek opgenomen)
Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
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.	Bijlage 1 bij bijlage III, bijlage VI
Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	Bijlage III

Maatregelen	Beleid
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.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
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.	Bijlage II, Bijlage XI, bijlage XII, auditbeleid (niet in handboek opgenomen)
Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiliging incidenten.	Bijlage XIII
Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Bijlage XIII
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.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)

5. Vertrouwelijkheid en integriteit

Maatregelen	Beleid
Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Autorisatiebeleid (niet in handboek opgenomen)
Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Autorisatiebeleid (niet in handboek opgenomen), Bijlage I
Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Autorisatiebeleid (niet in handboek opgenomen), Bijlage I
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.	Autorisatiebeleid (niet in handboek opgenomen), Bijlage I
Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	Autorisatiebeleid (niet in handboek opgenomen), Bijlage I
Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	Autorisatiebeleid (niet in handboek opgenomen), Bijlage I
Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie informatie houden aan de praktijk van de organisatie.	Bijlage III
Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	Bijlage I
Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	Autorisatiebeleid (niet in handboek opgenomen)
Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Er wordt gebruik gemaakt van tools om cryptografische sleutels tijdens hun gehele levenscyclus adequaat te beheren.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)

Maatregelen	Beleid
Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
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.	Bijlage XI, Bijlage XII
Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.	Bijlage III
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.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)

6. Controle en logging

Maatregelen	Beleid
Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Autorisatiebeleid (niet in handboek opgenomen)
Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	Taak beleggen op bestuursniveau, bijlage VI
Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	Auditbeleid (niet in handboek opgenomen)
De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Taakomschrijving ICT (intern dan wel extern te beleggen door bestuurder)
Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Bijlage VI, auditbeleid (niet in handboek opgenomen)
Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Bijlage VI, auditbeleid (niet in handboek opgenomen)