Toetsingskader digitaal Ondertekenen (pluscluster 9)

IBPDOC9

GEBRUIKERSGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Verantwoording

Met dank aan:

Leygraaf

Opdrachtgever:

Kennisnet / saMBO-ICT

Auteurs

Leo Bakker (Kennisnet)
Ludo Cuijpers (saMBO-ICT en Leeuwenborgh)

Versie 0.9, juli 2016

Sommige rechten voorbehouden

Inhoudsopgave

Verantwoording **2**

1. Inleiding **4**

1.1 Aanleiding 4

1.2 Uitgangspunten 4

1.2.1 De ondertekendienst: 4
1.2.2 De afnemer van de DigiD aansluiting (mbo instelling) 4

1.3 De praktijk 5

2. De impact voor de mbo instelling **6**

2.1 Het DigiD assessment in vogelvlucht 6

2.2 De stappen 6

2.2.1 Stap1, zelf toetsen a.d.h.v. de richtlijnen. 6
2.2.2 Stap 2, maatregelen treffen 7
2.2.3 Stap 3, audit uitvoeren 7
2.2.4 Stap 4, bevindingen naar Logius sturen 7

2.3 De scope 7

2.4 De DigiD normen 7

3. Toetsingskader Digid **9**

3.1 NOREA beveiligingsrichtlijnen voor mbo instellingen 9

3.2 Informatiebeveiliging statements ter onderbouwing NOREA beveiligingsrichtlijnen voor de instelling 10

3.3 NOREA beveiligingsrichtlijnen voor de dienstverlener 12

Bijlage 1: Framework informatiebeveiliging en privacy in het mbo 13

1. Inleiding

1.1 Aanleiding[1]

SaMBO-ICT, SION en Kennisnet voeren al enige tijd een verkenning uit naar de mogelijkheid tot het digitaal ondertekenen van de onderwijs- en praktijkovereenkomsten in het MBO (op basis van DigiD). Digitaal ondertekenen kan grote voordelen en besparingen opleveren, mits de impact en consequenties beheersbaar en betaalbaar zijn.
Op basis van de referentiearchitectuur onderwijs is een ontwerp van een ondertekendienst gemaakt (Edusign). Het ontwerp van de ondertekendienst vraagt (i.v.m. eisen ministerie en inspectie) niveau Stork-3[2] waardoor DigiD moet worden gehanteerd als authenticatiemiddel.
Op basis van dit ontwerp is door SURFmarket een offerteprocedure gestart voor de ondertekendienst.
De service provider Evidos is geselecteerd voor het leveren van de digitale ondertekendienst voor de POC (Proof Of Concept).
Logius[3] vereist dat een instelling die gebruikt maakt van een ondertekendienst met DigiD (voor studenten) jaarlijks een DigiD assessment laat uitvoeren. Daarbij wordt nagegaan of de webapplicatie en het beheer daaromheen voldoet aan een 28 tal door het Nationaal CyberSecurityCenter (NCSC) ontwikkelde richtlijnen voor beveiliging van webapplicaties.
Evidos heeft aangegeven een zogenaamde Third Party Mededeling (TPM) te kunnen afgeven, waarin ze aantoont te voldoen aan de DigiD normen..

1.2 Uitgangspunten

Onderstaande uitgangspunten beschrijven de reeds vastgestelde onderwerpen die voor het DigiD assessmenteen gegeven zijn. De impact van het DigiD-assessment voor de instellingen is dan ook op deze uitgangspunten gebaseerd.

1.2.1 De ondertekendienst:

- Verzorgt de tijdelijke opslag van het te ondertekenen document, de uitvoering van de (generieke) workflow rondom het verzamelen van de benodigde handtekeningen en het daadwerkelijke ondertekenen.
- Functioneert op STORK betrouwbaarheidsniveau 3 of vergelijkbaar.
- Maakt gebruik van DigiD (voor studenten), maar moet ook in staat zijn om andere authenticatiemiddelen te gebruiken, waaronder in ieder geval SURFconext en de Kennisnet Federatie (voor instellingen) en e-mail in combinatie met SMS codes (voor stagebedrijven).
- Kan rechtstreeks via het portal benaderd worden.
- Is in staat documenten in PDF formaat te ondertekenen.
- Is koppelbaar met bestaande Student Informatie Systemen SIS), die 'binnen de muren van de instelling' zorg dragen voor zaken als administratie en registratie, documentbeheer, zaakbeheer, en uitvoering van proces-specifieke workflow, logisch ontwerp.

1.2.2 De afnemer van de DigiD aansluiting (mbo instelling)

Indien een instelling afnemer is van de DigiD aansluiting dan dient deze te voldoen aan de aansluitvoorwaarden voor DigiD. Kernpunten daaruit zijn:

- Afnemer is zelf verantwoordelijk voor het bepalen van het gewenste Zekerheidsniveau voor zijn Afnemersdiensten (webdiensten).

---

[1] Bron VKA

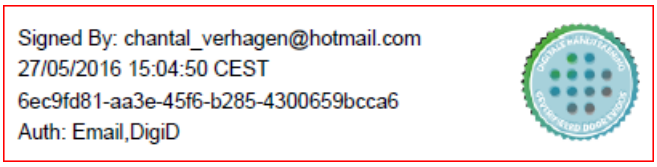
[2] *STORK QAA niveau 3*
Dit niveau vereist striktere methoden voor de verificatie van de geclaimde identiteit van de gebruiker. Deze moeten een hoge mate van zekerheid bieden. Middelenuitgevers moeten onder overheidstoezicht staan. Als type middel is 2-factor authenticatie vereist; gedacht kan worden aan 'soft' certificaten of one-time-passwords tokens.

[3] Logius is de dienst digitale overheid en onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De diensten en standaarden (o.a. DigiD) van Logius zijn voor de gehele overheid ontwikkeld. Logius is verantwoordelijk voor het beheer, de doorontwikkeling en de overheidsbrede toepassingen van deze diensten en standaarden.

- Afnemer is verplicht te voldoen en blijvend te voldoen aan de geldende “Norm ICT beveiligingsassessments DigiD”, en dit jaarlijks per DigiD aansluiting aan te tonen door middel van een verklaring die is afgegeven door een Register EDP-auditor. De periode waarin deze verklaring jaarlijks bij Logius dient te worden ingediend is van 1 januari tot 1 mei (art 5.5).
- Voor elke nieuwe aansluiting van Afnemer op de productieomgeving van DigiD dient binnen 2 maanden na aansluiting een aparte verklaring te worden ingediend. De eerstvolgende verklaring dient te worden ingediend conform de regeling in artikel 5.5, met dien verstande dat in de eerste 12 maanden na aansluiting hooguit eenmaal een verklaring hoeft te worden ingediend.
- Een in het kader van het DigiD assessment afgegeven Third Party Mededeling is maximaal 12 maanden geldig en kan slechts eenmaal gebruikt worden.
- De kosten voor het DigiD assessment en de verklaring komen volledig voor rekening van Afnemer.
- Indien uit de verklaring blijkt dat niet of niet volledig wordt voldaan aan de geldende “Norm ICT-beveiligingsassessments DigiD” heeft Logius het recht zonder aankondiging vooraf de levering van DigiD op te schorten. (In de praktijk zendt Logius eerst een verzoek tot opstellen van een Verbeterplan en vraagt om binnen een nader te bepalen termijn een her-audit te doen op doorgevoerde verbeteringen.)

1.3 De praktijk

Medio 2016 is de eerste pilot bij ROC De Leijgraaf succesvol afgerond. Van de 300 studenten ondertekende 95% op tijd. Een digitaal ondertekende OOK laat onderstaande ondertekening zien:



De procedure is als volgt:

1. Een deelnemer meldt zich aan.
2. De deelnemer wordt uitgenodigd voor een intake en wordt vervolgens geplaatst.
3. De deelnemersadministratie maakt de OOK aan en stuurt een pdf plus e-mail adres van de deelnemer naar de dienstverlener.
4. De deelnemer ondertekent de OOK d.m.v. DigiD.
5. De dienstverlener stuurt de ondertekende OOK terug naar de mbo instelling.

2. De impact voor de mbo instelling

2.1 Het DigiD assessment in vogelvlucht

Instellingen zijn en blijven eigenaar van de gegevens in de ondertekendienst. Een instelling moet over deze gegevens kunnen beschikken wanneer dit nodig blijkt. De instelling is verantwoordelijk voor de risicobeheersing en beveiliging van de elektronische dienstverlening. De instelling die gebruik maakt van de ondertekendienst met DigiD dient jaarlijks een DigiD assessment uit te laten voeren.
Een dienstverlener biedt een ondertekendienst, bijvoorbeeld “Ondertekenen.nl” aan. Hiervoor is ten behoeve van de instellingen door SURFmarket een bemiddelingsovereenkomst **met** een Juridisch Normenkader Cloudservices Hoger Onderwijs met de dienstverlener gesloten. In de bemiddelingsovereenkomst is opgenomen dat de dienstverlener voldoet aan beveiligingseisen en een TPM (“Third Party Memorandum”) over haar dienstverlening oplevert. SURFmarket en de dienstverlener hebben aangegeven in nadere afspraken vast te leggen dat de dienstverlener jaarlijks een DigiD assessment rapport oplevert over haar DigiD dienstverlening (een zogenaamd “DigiD TPM”) (zie 3.4).

De bemiddelingsovereenkomst geeft de algemene voorwaarden aan voor de levering van de ondertekendienst. De instelling sluit op basis van de bemiddelingsovereenkomst zelf een gebruikersovereenkomst af met de dienstverlener waarmee de algemene voorwaarden van toepassing worden verklaard op de dienstverlening aan de instelling. Deze overeenkomsten vormen in opzet een goede basis voor het DigiD assessment.

De instelling dient ook zelf aan een aantal DigiD normen te voldoen. Een aantal maatregelen om aan deze normen te voldoen wordt ook beoordeeld in het onderzoek dat in het kader van de jaarrekeningcontrole door de accountant wordt uitgevoerd naar de geautomatiseerde informatiesystemen. Doel daarvan is vast te stellen of voldoende algemene maatregelen binnen de (automatiserings-)organisatie zijn genomen om de betrouwbare en continue werking van de geautomatiseerde informatiesystemen te waarborgen. (Zie 3.1 en 3.2).

2.2 De stappen

Het stappenplan omvat 4 stappen voor het uitvoeren van een DigiD assessment.

2.2.1 Stap1, zelf toetsen a.d.h.v. de richtlijnen.

In deze stap wordt een proefaudit uitgevoerd met de volgende resultaten. De proefaudit kan door (de auditor van) de instelling zelf uitgevoerd worden of door de DigiD auditor. Indien het DigiD assessment voor het eerst wordt uitgevoerd dan wordt deze stap dringend geadviseerd. Bij vervolg assessments kan deze stap, indien er weinig wijzigingen in de processen en organisatie zijn geweest, worden overgeslagen.

1. Bepalen scope en verdeling DigiD verantwoordelijkheid
   Resultaat: Inzicht in de verdeling van verantwoordelijkheden tussen de instelling en de IT leveranciers. Inzicht in welke normen door de instelling zelf worden ingevuld.
2. Voorbereiding proefaudit
   Resultaat: Voor de interviews zijn de juiste personen bekend en te bestuderen documentatie is beschikbaar. Interviewpartners zijn voorbereid. De interviews zijn ingepland.
3. Uitvoeren proefaudit
   Resultaat: De uitkomsten van de proefaudit bestaan uit bevindingen en aanbevelingen over de mate waarin de maatregelen in de instelling in overeenstemming zijn met de vereisten van de DigiD norm.
4. Presenteren resultaten
   Resultaat: Een presentatie waarin op managementniveau inzicht geboden wordt in de achtergrond en aanleiding van de DigiD audit, de mate van conformiteit aan de normen voor de DigiD audit, de mate waarin aangesloten kan worden op de reguliere accountantscontrole, sterkten en zwakten en benodigde vervolgacties.

2.2.2 Stap 2, maatregelen treffen

In deze stap worden eventuele tekortkomingen aangepakt. Nagegaan wordt welke maatregelen de hoogste prioriteit hebben en hoe snel en met welke diepgang de verbeteringen moeten worden doorgevoerd. Adviseurs kunnen de instelling adviseren bij deze stap.
Resultaat: Verbeterde beveiligingsmaatregelen met in acht name van het ambitieniveau van de instelling.

2.2.3 Stap 3, audit uitvoeren

In deze stap voert de auditor de feitelijke DigiD audit uit conform de auditprotocollen zoals deze geldig zijn. Dit dient plaats te vinden door een door de NOREA gecertificeerde Register EDP auditors (RE). De auditor bestudeert de documentatie en houdt interviews. De auditor beoordeelt de opzet (documentatie) en het bestaan (feitelijk uitgevoerde activiteiten) en velt een oordeel per norm, met een gedetailleerde onderbouwing van de argumentatie. De werking, het uitvoeren van beheersmaatregelen over een langere periode, wordt niet getoetst. De auditor toetst de auditrapportage van de leverancier aan de algemene richtlijnen voor de rapportage over DigiD audits en op de volledigheid van de overeengekomen te toetsen normen. De bevindingen legt de auditor vast in een rapportage.
Resultaat: DigiD assessment rapportage, bestaande uit:
1. totaaloverzicht van de scores per norm, maar geen samenvattend oordeel;
2. per norm een uitspraak of de interne beheersingsmaatregelen, - in audit termen - 'in alle van materieel belang zijnde aspecten, op afdoende wijze qua opzet en bestaan zijn ingeregeld';
3. per norm een toelichting op de uitspraak en eventueel voorstellen voor verbetering;
4. een beschrijving van de onderzochte dienst en de betrokken leveranciers

Resultaat: Uitgevoerde DigiD assessment, leidend tot een auditrapport welke voldoet aan de eisen van Logius.

2.2.4 Stap 4, bevindingen naar Logius sturen

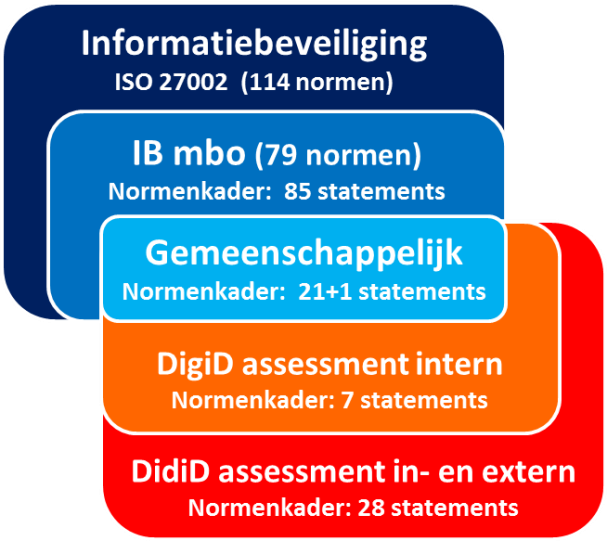
Het rapport van de auditor en het TPM rapport van de it service organisatie worden door de instelling aangeboden aan Logius. Logius zendt vervolgens haar reactie terug aan de instelling. Indien niet aan alle DigiD normen wordt voldaan, dan zal Logius om een verbeterplan vragen. Soms vraagt Logius bij onduidelijkheden om een nadere toelichting van de auditor.

2.3 De scope

Het DigiD assessment is gericht op de ‘webfacing’ onderdelen van de digitale dienstverlening aan burgers. Voor de ondertekendienst houdt dit in dat het object van onderzoek is de web omgeving van de DigiD aansluiting. Het onderzoek richt zich op de webapplicatie, de URL’ s waarmee deze kunnen worden benaderd, de infrastructuur (binnen de DMZ waar webapplicaties zich bevinden) en een aantal ondersteunende processen conform de “Norm ICT-beveiligingsassessments DigiD” van Logius.

2.4 De DigiD normen

De normen voor het DigiD assessment zijn een subset van 28 beveiligingsrichtlijnen uit de Nationaal Cyber Security Centrum (NCSC) richtlijn. De normen betreffen de governance, het applicatie- en infrastructuurbeheer van de ondertekendienst bij de instelling en de serviceprovider.
Zo levert Evidos bijvoorbeeld naar verwachting een TPM op waarin alle 28 DigiD normen zijn opgenomen. Een aandachtspunt is nog B0-13. Aanvankelijk was deze norm niet door Evidos opgenomen. De norm vereist dat ook de serviceprovider maatregelen treft om op een gecontroleerde wijze websites te verwijderen. Evidos heeft aangegeven bij deze norm zelf een procedure te zullen hanteren voor het op een gecontroleerde wijze verwijderen van een website. Evidos geeft tevens aan welke normen bij de instelling getoetst moeten worden. Deze komen overeen met de normen die vanuit Logius met betrekking tot de DigiD assessment zijn aangegeven om bij de instelling getoetst te worden. Evidos heeft aangegeven de TPM binnen 2 maanden na live gaan van de dienst te kunnen opleveren.



De instelling is zelf verantwoordelijk voor 7 DigiD normen. Tevens is aangegeven welke norm in de bemiddelingsovereenkomst en het Juridische Normenkader Cloudservices Hoger Onderwijs met Evidos is belegd. Indien de instelling op basis van deze bemiddelingsovereenkomst een gebruikersovereenkomst sluit met Evidos, dan is daarmee norm B0-14 (Leg afspraken met leveranciers vast in een overeenkomst.) afdoende afgedekt.
Enkele van deze normen kunnen ook als onderdeel van de jaarrekeningcontrole door de accountant zijn onderzocht. De accountantscontrole is onder andere gericht op het vaststellen van de betrouwbaarheid van de financiële informatie/verslaggeving van de instelling. Aangezien deze financiële informatie in de meeste gevallen rechtstreeks afkomstig is uit geautomatiseerde informatiesystemen, is de betrouwbare en continue werking van die systemen van direct belang voor de jaarrekeningcontrole. Het doel van het onderzoek naar de geautomatiseerde informatiesystemen is om vast te stellen of voldoende algemene maatregelen binnen de (automatiserings-)organisatie zijn genomen om de betrouwbare en continue werking van de geautomatiseerde informatiesystemen te waarborgen (de zogenaamde General Computer Controls; GCC).

In hoofdstuk 3 worden de NOREA beveiligingsrichtlijnen gekoppeld aan het Toetsingskader ib voor het mbo (IBP-DOC3). 6 van de 7 NOREA statements wordt door 22 ISO 27002 statements afgedekt. Omdat 1 statement (wachtwoordbeleid) niet in het toetsingskader ib is opgenomen is dit alsnog toegevoegd.
Het 7e NOREA statement (B 0-13) wordt alsnog door Evidos afgedekt.

3. Toetsingskader DigiD

3.1 NOREA beveiligingsrichtlijnen voor mbo instellingen

NOREA Referentie	Beveiligingsrichtlijn	Mbo nummer	ISO norm
B 0-12	Ontwerp en richt maatregelen in met betrekking tot toegangsbeveiliging / toegangsbeheer.	5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8 5.9 Niet in gebruik	9.1.1 9.1.2 9.2.1 9.2.2 9.2.3 9.2.4 9.3.1 9.4.1 9.4.2 **9.4.3**
	Toelichting: op basis van inspectie wordt vastgesteld of er een procedure aanwezig is voor toegangsbeveiliging / toegangsbeheer en formele richtlijnen rondom wachtwoordinstellingen, beheeraccounts en shared accounts. Wachtwoorden moeten een looptijd hebben van maximaal 3 maanden en een complexiteit van 8 tekens, waarvan tenminste 1 hoofdletter, 1 cijfer en 1 diakritisch (leesteken etc.) teken en 1 kleine letter.		
B 0-13	Niet (meer) gebruikte websites en/of informatie moet worden verwijderd.	geen	geen
	Het registreren van websites is afdoende.		
B 0-14	Leg afspraken met leveranciers vast in een overeenkomst.	1.15 4.11	15.1.2 15.2.2
	Met de leverancier moeten afspraken worden vastgelegd in een formele overeenkomst. Bovendien moet er een **A**lgemene **D**ienst**V**erlenings**O**vereenkomst (ADVO) en bewerkersovereenkomst worden afgesloten.		
B 2-1	Maak gebruik van beheermechanismen		
	Cluster 3 en 4 van het mbo toetsingskader ibp moet op voldoende niveau zijn.		
B 5-1	Voer sleutelbeheer in waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers te vinden zijn.	1.9 en 1.10 5.10 en 5.11	10.1.1 10.1.2
	Wachtwoorden en sleutels worden beveiligd opgeslagen. Er is wachtwoord benodigd om bij de locatie, waar de sleutels behorende bij de SSL certificaten zijn opgeslagen, te komen.		
B 5-3	Sla gevoelige gegevens versleuteld of gehashed op (voor zover betrekking hebbend op DigiD).	1.9 en 1.10 5.10 en 5.11	10.1.1 10.1.2
	Gevoelige gegevens worden versleuteld opgeslagen.		
B 7-9	Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en response inzake informatiebeveiliging dienen adequaat te zijn vastgesteld.	1.1 en 1.2 1.3 1.4	5.1.1 5.1.2 6.1.1
	Een goedgekeurd en gecommuniceerd ibp beleidsplan moet aanwezig zijn. Dit beleidsplan moet in een PDCA cyclus zijn opgenomen.		

3.2 Informatiebeveiliging statements ter onderbouwing NO-REA beveiligingsrichtlijnen voor de instelling

Bij B0-12 moeten de volgende statements uit het mbo toetsingskader informatiebeveiliging en privacy in acht genomen worden:

Nr.	ISO27002	Statement
5.1	9.1.1	**Beleid voor toegangsbeveiliging:** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.
5.2	9.1.2	**Toegang tot netwerken en netwerkdiensten:** Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
5.3	9.2.1	**Registratie en afmelden van gebruikers:** Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
5.4	9.2.2	**Gebruikers toegang verlenen:** Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
5.5	9.2.3	**Beheren van speciale toegangsrechten:** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.
5.6	9.2.4	**Beheer van geheime authenticatie-informatie van gebruikers:** Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.
5.7	9.3.1	**Geheime authenticatie-informatie gebruiken:** Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie informatie houden aan de praktijk van de organisatie.
5.8	9.4.1	**Beperking toegang tot informatie:** Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.
5.9	9.4.2	**Beveiligde inlogprocedures:** Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.

Opvallend is dat er 1 statement is dat niet in het mbo toetsingskader is opgenomen maar waar wel in het kader van de Digid audit op wordt getoetst. En dat is het systeem voorwachtwoordenbeheer. Het verdient daarom aanbeveling om deze als extra statement hier op te nemen (vandaar de 21 + 1 in het plaatje)

9.4.3 Systeem voor wachtwoordbeheer (ISO 27002-2013)

Beheersmaatregel

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

Implementatierichtlijn

Een systeem voor wachtwoordbeheer behoort:

a) het gebruik van individuele gebruikersidentificaties en wachtwoorden af te dwingen om de toerekenbaarheid te handhaven;
b) gebruikers de mogelijkheid te bieden hun eigen wachtwoord te kiezen en te wijzigen, en een bevestigingsprocedure te bevatten die rekening houdt met foutieve invoer;
c) de keuze voor sterke wachtwoorden af te dwingen;
d) gebruikers te dwingen hun wachtwoord bij het eerste inloggen te wijzigen;
e) wijziging van het wachtwoord periodiek en telkens wanneer dat nodig is af te dwingen;
f) een registratie van eerder gebruikte wachtwoorden bij te houden en te voorkomen dat deze opnieuw worden gebruikt;
g) wachtwoorden niet op het scherm te tonen als ze worden ingevoerd;
h) wachtwoordbestanden apart van systeem gegevens van toepassingen op te slaan;
i) wachtwoorden in beschermde vorm op te slaan en te versturen.

Overige informatie

Sommige toepassingen vereisen dat gebruikerswachtwoorden door een onafhankelijke instantie worden toegekend; in dergelijke gevallen zijn de punten b), d) en e) van bovenstaande richtlijn niet van toepassing. In de meeste gevallen worden wachtwoorden door de gebruiker gekozen en onderhouden.

Bij B0-13 en B0-14 zijn de volgende statements uit het mbo toetsingskader ibp van toepassing:

Nr.	ISO27002	Statement
1.15	15.1.2	**Opnemen van beveiligingsaspecten in leveranciersovereenkomsten**: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.
4.11	15.2.2	**Beheer van veranderingen in dienstverlening van leveranciers:** Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.

Bij B2-1 zijn eigenlijk de hele clusters 3 en 4 van het mbo toetsingskader van toepassing.
Bij B5-1 en B5-2 zijn de volgende statements uit het mbo toetsingskader van toepassing:

Nr.	ISO27002	Statement
1.9	10.1.1.1	**Beleid inzake het gebruik van cryptografische beheersmaatregelen**: Ter bescherming van informatie behoort een beleid voor het gebruik van crypto grafische beheersmaatregelen te worden ontwikkeld.
1.10	10.1.1.2	**Beleid inzake het gebruik van cryptografische beheersmaatregelen:** Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van crypto grafische beheersmaatregelen wordt geïmplementeerd.
5.10	10.1.2.1	**Sleutelbeheer:** Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld.
5.11	10.1.2.2	**Sleutelbeheer:** Er wordt gebruik gemaakt van tools om cryptografische sleutels tijdens hun gehele levenscyclus adequaat te beheren.

Tot slot zijn bij B7-9 de volgende statements uit het mbo toetsingskader van toepassing:

Nr.	ISO27002	Statement
1.1	5.1.1.1	**Beleidsregels voor informatiebeveiliging**: Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur.
1.2	5.1.1.2	**Beleidsregels voor informatiebeveiliging**: Het door het bestuur vastgestelde Informatiebeveiligingsbeleid wordt gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
1.3	5.1.2	**Beoordeling van het Informatiebeveiligingsbeleid**: Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
1.4	6.1.1	**Taken en verantwoordelijkheden informatiebeveiliging**: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen

3.3 NOREA beveiligingsrichtlijnen voor de dienstverlener

NOREA Referentie	Beveiligingsrichtlijn	Oordeel
B 0-5	Alle wijzigingen worden altijd eerst getest voordat deze in productie worden genomen en worden via wijzigingsbeheer doorgevoerd.	Audit uitgevoerd bij Dienstverlener
B 0-6	Maak gebruik van een hardeningsproces, zodat alle ICT-componenten zijn gehard tegen aanvallen.	Audit uitgevoerd bij Dienstverlener
B 0-7	laatste (beveiligings)patches zijn geïnstalleerd en deze worden volgens een patchmanagement proces doorgevoerd.	Audit uitgevoerd bij Dienstverlener
B 0-8	Penetratietests worden periodiek uitgevoerd.	Audit uitgevoerd bij Dienstverlener
B 0-9	Vulnerability assessments (security scans) worden periodiek uitgevoerd.	Audit uitgevoerd bij Dienstverlener
B 1-1	Er moet gebruik worden gemaakt van een Demilitarised Zone (DMZ), waarbij compartimentering wordt toegepast en de verkeersstromen tussen deze compartimenten wordt beperkt tot alleen de hoogst noodzakelijke.	Audit uitgevoerd bij Dienstverlener
B 1-2	Beheer- en productieverkeer zijn van elkaar gescheiden.	Audit uitgevoerd bij Dienstverlener
B 1-3	Netwerktoegang tot de webapplicaties is voor alle gebruikersgroepen op een zelfde wijze ingeregeld.	Audit uitgevoerd bij Dienstverlener
B 3-1	De webapplicatie valideert de inhoud van een HTTP-request voor die wordt gebruikt.	Audit uitgevoerd bij Dienstverlener
B 3-2	De webapplicatie controleert voor elk HTTP verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft.	Audit uitgevoerd bij Dienstverlener
B 3-3	De webapplicatie normaliseert invoerdata voor validatie.	Audit uitgevoerd bij Dienstverlener
B 3-4	De webapplicatie codeert dynamische onderdelen in de uitvoer.	Audit uitgevoerd bij Dienstverlener
B 3-5	Voor het raadplegen en/of wijzigen van gegevens in de database gebruikt de webapplicatie alleen geparametriseerde queries.	Audit uitgevoerd bij Dienstverlener
B 3-6	De webapplicatie valideert alle invoer, gegevens die aan de webapplicatie worden aangeboden, aan de serverzijde.	Audit uitgevoerd bij Dienstverlener
B 3-7	De webapplicatie staat geen dynamische file includes toe of beperkt de keuze mogelijkheid (whitelisting).	Audit uitgevoerd bij Dienstverlener
B 3-15	Een (geautomatiseerde) blackbox scan wordt periodiek uitgevoerd.	Audit uitgevoerd bij Dienstverlener
B 3-16	Zet de cookie attributen ‘HttpOnly’ en ‘Secure’.	Audit uitgevoerd bij Dienstverlener
B 5-2	Maak gebruik van versleutelde (HTTPS) verbindingen.	Audit uitgevoerd bij Dienstverlener
B 5-4	Versleutel cookies.	Audit uitgevoerd bij Dienstverlener
B 7-1	Maak gebruik van Intrusion Detection Systemen (IDS).	Audit uitgevoerd bij Dienstverlener
B 7-8	Voer actief controles uit op logging.	Audit uitgevoerd bij Dienstverlener

Bijlage 1: Framework informatiebeveiliging en privacy in het mbo