**Handboek mbo-audits:**

 **normenkader ib**

 **compliance-kader privacy**

 **normenkader examineren**

 **normenkader digitaal ondertekenen**

 **versie 3.0, september 2017**

****

**IBPDOC21**

Inhoudsopgave

[1. Normenkader informatiebeveiliging (cluster 1 t/m 6) 3](#_Toc460623627)

[1.1 Cluster beleid en organisatie 5](#_Toc460623628)

[1.2 Personeel, studenten en gasten 8](#_Toc460623629)

[1.3 Ruimtes en apparatuur 9](#_Toc460623630)

[1.4 Continuïteit 11](#_Toc460623631)

[1.5 Toegangsbeveiliging en integriteit 13](#_Toc460623632)

[1.6 Controle en logging 15](#_Toc460623633)

[2. Compliance-kader privacy 16](#_Toc460623634)

[2.1 Basis privacy principes 16](#_Toc460623635)

[2.1.1 Privacy by design 16](#_Toc460623636)

[2.1.2 Doel en doelbinding 16](#_Toc460623637)

[2.1.3 Grondslag 17](#_Toc460623638)

[2.1.4 Dataminimalisatie 17](#_Toc460623639)

[2.1.5 Transparantie 17](#_Toc460623640)

[2.1.6 Rechten van de betrokkene 17](#_Toc460623641)

[2.1.7 Beveiliging 18](#_Toc460623642)

[2.1.8 Datakwaliteit (data-integriteit) 18](#_Toc460623643)

[2.1.9 Verantwoordelijkheid (responsibility) 18](#_Toc460623644)

[2.1.10 Eigendom 18](#_Toc460623645)

[2.2 Statements compliance-kader privacy 19](#_Toc460623646)

[2.2.1 Beleid en organisatie 19](#_Toc460623647)

[2.2.2 Personeel, studenten en gasten 22](#_Toc460623648)

[2.2.3 Ruimtes en apparatuur 24](#_Toc460623649)

[2.2.4 Vertrouwelijkheid en integriteit 24](#_Toc460623650)

[2.2.5 Controle en logging 25](#_Toc460623651)

[2.3 Statements gemeenschappelijk normenkader 26](#_Toc460623652)

[2.3.1 Cluster 1: Beleid en organisatie 26](#_Toc460623653)

[2.3.2 Cluster 2: Personeel, studenten en gasten 27](#_Toc460623654)

[2.3.3 Cluster 3: Ruimtes en apparatuur 27](#_Toc460623655)

[2.3.4 Cluster 4: Continuïteit 28](#_Toc460623656)

[2.3.5 Cluster 5: Vertrouwelijkheid en integriteit 28](#_Toc460623657)

[2.3.6 Cluster 6: Controle en logging 29](#_Toc460623658)

[3. Normenkader examinering 30](#_Toc460623659)

[3.1 Basisprincipes examinering 31](#_Toc460623660)

[3.2 Statements normenkader examinering 31](#_Toc460623661)

[3.2.1 Dit beleid is afgeleid van het document Kwaliteitsborging Examineren. 31](#_Toc460623662)

[3.2.2 Aanvullende statements gerelateerd aan personeel 32](#_Toc460623663)

[3.2.3 Aanvullende statements gerelateerd aan uitvoering 32](#_Toc460623664)

[3.3 Statements examinering afgeleid van het ib normenkader 33](#_Toc460623665)

[3.3.1 Generieke statements voorafgaande aan examinering 33](#_Toc460623666)

[3.3.2 Generieke statements tijdens het proces van examinering 33](#_Toc460623667)

[4. Normenkader digitaal ondertekenen 35](#_Toc460623668)

[4.1 Basisprincipes digitaal ondertekenen 35](#_Toc460623669)

[4.2 Statements DigiD 36](#_Toc460623670)

[4.2.1 NOREA-beveiligingsrichtlijnen voor mbo-instellingen 36](#_Toc460623671)

[4.2.2 NOREA-beveiligingsrichtlijnen voor Evidos 37](#_Toc460623672)

[4.3 Informatiebeveiliging-statements ter onderbouwing NOREA-beveiligingsrichtlijnen voor de instelling 38](#_Toc460623673)

[Verantwoording 41](#_Toc460623674)

# Normenkader informatiebeveiliging (cluster 1 t/m 6)

Auditing is het controleren van een (deel van) een organisatie. 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.



**MBOaudit** hanteert als uitgangspunt het generieke internationale normenkaders voor informatiebeveiliging ISO27001/ISO 27002 (versie 2013). De Nederlandse versie van dit normenkader staat bekend als de ‘Code voor Informatiebeveiliging’. De mbo-sector heeft de ISO 27002 normen een subset van 79 normen overgenomen. Zes statements zijn gesplitst, zodat in totaal 85 statements worden gebruikt. Het normenkader wordt verrijkt tot een toetsingskader door er bewijslast aan toe te voegen. Ook is het normenkader ingedeeld in thematische clusters.

**Clustering naar zes thema’s**

Het normenkader informatiebeveiliging bevat 85 statements verdeelt over 6 clusters. De clustering is gebaseerd op een logische indeling die aansluit bij de bedrijfsvoering van het mbo-onderwijs.

|  |  |  |
| --- | --- | --- |
| **Cluster** | **Onderwerpen (o.a.)** | **Aantal statements** |
| 1. Beleid en organisatie
 | InformatiebeveiligingsbeleidClassificatieInrichten beheer | 21 statements |
| 1. Personeel, studenten en gasten
 | InformatiebeveiligingsbeleidAanvullingen arbeidsovereenkomstScholing en bewustwording | 7 statements |
| 1. Ruimtes en apparatuur
 | Beveiligen van hardware, devices en bekabeling | 15 statements |
| 1. Continuïteit
 | Anti virussen, back up, bedrijfscon­tinuïteit planning | 15 statements |
| 1. Toegangsbeveiliging en integriteit
 | Gebruikersbeheer, wachtwoorden, online transacties, sleutelbeheer, validatie | 17 statements |
| 1. Controle en logging
 | Systeemacceptatie, loggen van gegevens, registreren van storingen, toetsen beleid | 10 statements |

**Kwaliteitsaspecten informatiebeveiliging**

Het toetsingskader hanteert de gangbare kwaliteitsaspecten van informatiebeveiliging: beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. De kwaliteitsaspecten effectiviteit en efficiëntie worden verder niet besproken. In een financiële ict-benchmark worden deze onderzocht, maar niet in de **MBOaudit.**.

De gebruikte kwaliteitsaspecten volgen strikte definities en zijn niet vrij te interpreteren.

**Beschikbaarheid:** de mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening waarborgen.

Deelaspecten hiervan zijn:

* continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is;
* portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is;
* herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

**Integriteit:** de mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de ict-dienstverlening waarborgen.

Deelaspecten hiervan zijn:

* juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in ict-systemen ten opzichte van de werkelijkheid is gerealiseerd;
* volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
* tijdigheid: de mate van zekerheid dat de gegevens op het juiste tijdstip beschikbaar zijn;
* waarborging: de mate waarin de correcte werking van de ict-processen is gewaarborgd.

**Vertrouwelijkheid:** de mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.

Deelaspecten hiervan zijn:

* autorisatie:de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is;
* authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is;
* identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn;
* periodieke controle op de bestaande bevoegdheden: het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

**Controleerbaarheid:** de mogelijkheid om kennis te verkrijgen over de structurering (documentatie) en werking van de ict-dienstverlening.

Deelaspecten hiervan zijn:

* testbaarheid: de mate waarin de integere werking van de IT-dienstverlening te testen is;
* meetbaarheid: de mate waarin meet- en controlepunten aanwezig voldoende aanwezig zijn;
* verifieerbaarheid: de mate waarin de integere werking van een IT-dienstverlening te verifiëren is.

**Bewijsvoering en volwassenheidsniveaus**

Het **Capability Maturity Model** is een model dat aangeeft op welk volwassenheidsniveau de informatievoorziening van een organisatie zit. Door ervaring in het gebruik is gebleken dat dit model op diverse processen in de organisatie toepasbaar is, ook op informatiebeveiliging. De volgende volwassenheidsniveaus worden gehanteerd voor de bewijslast:

|  |  |
| --- | --- |
| Volwassenheidsniveau 1 (Adhoc / initieel) | Initial: op dit niveau is de aanpak chaotisch en ad hoc. Problemen worden pas opgelost als ze zich voordoen. Dit is het niveau dat iedere organisatie aankan. |
| Volwassenheidsniveau 2(haalbaar maar intuïtief) | Repeatable: is het niveau waarbij de organisatie zover geprofessionaliseerd is (bijvoorbeeld door het invoeren van projectmanagement) dat bij het ontwikkelproces gebruik wordt gemaakt van de kennis die eerder is opgedaan. Beslissingen worden dus genomen op basis van ervaring. |
| Volwassenheidsniveau 3(gedefinieerd proces) | Defined: is het niveau waarbij de belangrijkste processen zijn gestandaardiseerd. *Een en ander is vastgelegd en daardoor controleerbaar (toevoeging ho).* |
| Volwassenheidsniveau 4(beheerst en meetbaar) | Managed: is het niveau waarbij de kwaliteit van het ontwikkelproces wordt gemeten zodat het kan worden bijgestuurd. *Een PDCA cyclus wordt aantoonbaar doorlopen (toevoeging HO).* |
| Volwassenheidsniveau 5(geoptimaliseerd) | Optimised: is het niveau waarbij het ontwikkelproces als een geoliede machine loopt en er alleen maar sprake is van fijn afstemming (de puntjes op de i). |

**Update naar toetsingskader mbo versie 3.0**

Het toetsingskader ibp in het mbo is in de zomer van 2017 bijgewerkt om een aantal statements te verduidelijken. Er zijn geen wijzigingen in de statements als zodanig aangebracht maar er zijn tips toegevoegd om de interpretatie ervan scherper te maken. Deze tips van versie 3.0 zijn aan de statements van cluster 1 t/m 6 hieronder in de gele vlakken toegevoegd.

## Cluster beleid en organisatie

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **1.1** | **5.1.1.1** | Beleidsregels voor informatiebeveiliging: Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur. |
|  |  | **Tips:** Hanteer de "Leidraad Informatiebeveiligingsbeleid XX-V2.0" als uitgangspunt. Controleer het beleid voor de volgende onderdelen op aanwezigheid en juistheid:1. [Inleiding](#_Toc437252188)
2. [Beleidsuitgangspunten en -principes informatiebeveiliging en privacy](#_Toc437252194)
3. [Classificatie](#_Toc437252198)
4. [Wet- en regelgeving](#_Toc437252199)
5. [Governance informatiebeveiligingsbeleid](#_Toc437252208)

[Melding en afhandeling van incidenten](#_Toc437252224) |
| **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. |
|  |  | **Tips:** onderzoek of er ook met externe partijen wordt gecommuniceerd over het informatiebeveiligings- en privacybeleid van de instelling. Zie ook de SCIPR “Leidraad Informatiebeveiligingsbeleid XX-V2.0.docx”. |
| **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. |
|  |  | **Tips:** het beleid is onderdeel geworden van de PDCA-cyclus. Achterhaal op basis van interviews of dit gerealiseerd is. |
| **1.4** | **6.1.1** | Taken en verantwoordelijkheden informatiebeveiliging: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen |
|  |  | **Tips:** Hanteer de "Leidraad Informatiebeveiligingsbeleid XX-V2.0" als uitgangspunt. Controleer de volgende onderdelen op aanwezigheid en juistheid:1. [Inleiding](#_Toc437252188)
2. [Beleidsuitgangspunten en -principes informatiebeveiliging en privacy](#_Toc437252194)
3. [Classificatie](#_Toc437252198)
4. [Wet- en regelgeving](#_Toc437252199)
5. [**Governance informatiebeveiligingsbeleid**](#_Toc437252208)
6. [Melding en afhandeling van incidenten](#_Toc437252224)

Onderzoek of de governance ook vertaald is in een organogram. |
| **1.5** | **6.1.5** | Informatiebeveiliging in projectbeheer: Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project. |
|  |  | **Tips:** Als onderdeel van een project worden de volgende aandachtspunten meegenomen:* De IBP[[1]](#footnote-1) manager wordt in een vroeg stadium betrokken bij het project.
* Er wordt een IBP-paragraaf opgenomen in het project.
* Er wordt een BIV/PIA uitgevoerd.

Dit is de operationele uitvoer van, bijvoorbeeld, een aanbesteding of een project in het kader van life-cycle management. Zie ook 3.1.14. |
| **1.6** | **6.2.1.1** | Beleid voor mobiele apparatuur: Er dient beleid te worden vastgesteld om de risico’s die het gebruik van mobiele apparatuur met zich meebrengt te beheren. |
|  |  | **Tips:** Er is een beleid op het gebied van Bring Your Own Device (BYOD) en Bring Your Company Device (BYCD). Bovendien wordt dit beleid gecontroleerd. |
| **1.7** | **8.2.1** | Classificatie van informatie: Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging. |
|  |  | **Tips:** er is een beleid waarin de uitgangspunten van de BIV classificatie worden beschreven. De classificaties wordt op Laag, Midden en Hoog niveau beschreven. De beheersmaatregelen worden eveneens op deze schaalverdeling beschreven. Deze classificatie wordt gebruikt en periodiek geëvalueerd. |
| **1.8** | **8.2.2** | Informatie labelen: Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie. |
|  |  | **Tips:** de instelling moet kunnen aantonen dat de classificatie daadwerkelijk wordt toegepast. Te denken valt aan:* Security architectuur document;
* Documenten die voorzien zijn van een ‘stempel’ vertrouwelijk;
* Aanwezigheid van een vertrouwenspersoon;
* Aanvullende afspraken voor functioneel beheerders i.v.m. vertrouwelijkheid;

Etc. |
| **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. |
|  |  | **Tips:** Er is een beleid t.a.v. cryptografische beheersmaatregelen. |
| **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. |
|  |  | **Tips:** de instelling heeft een of meerder tools aangeschaft in het kader van cryptografische beheersmaatregelen.  |
| **1.11** | **11.2.5** | Verwijdering van bedrijfsmiddelen: Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring. |
|  |  | **Tips:** apparatuur mag worden meegenomen naar huis. De medewerker gaat akkoord (tekent) met een computerreglement of een Acceptable User Policy (AUP). |
| **1.12** | **13.2.1** | Beleid en procedures voor informatietransport: Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn. |
|  |  | **Tips:** de instelling heeft een beleid vastgesteld waarin bepaald wordt onder welke voorwaarden er informatie met andere partijen mag worden uitgewisseld. (zie Bijlage 1 Beleid en procedures voor informatietransport). |
| **1.13** | **13.2.2** | Overeenkomsten over informatietransport: Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen. |
|  |  | **Tips:** er worden contracten en bewerkersovereenkomsten met leveranciers afgesloten waarmee informatie wordt uitgewisseld. Het betreft hier zowel het transport van fysieke documenten (aangetekende stukken) als van digitale informatie. |
| **1.14** | **14.1.1** | Analyse en specificatie van informatiebeveiligingseisen: De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen. |
|  |  | **Tips:** er is beleid dat gebruik kan worden in een programma van eisen bij een aanbesteding. BIV en PIA kunnen hier een onderdeel van zijn. Aanbesteding en life cycle. Systeemeigenaar (proceseigenaar) is verantwoordelijk.De ICT afdeling is belast met de implementatie. Zie ook hoofdstuk 3.1.5 Informatiebeveiliging in projectbeheer |
| **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. |
|  |  | **Tips:** Toegang van systemen door externe medewerkers op het netwerk op de eigen locatie. Beveiligingsaspecten in de meest brede zin. 1. Omschrijving van de informatie die moet worden verschaft of toegankelijk moet worden en van de methoden om de informatie te verschaffen of toegankelijk te maken;
2. Classificatie van de informatie in overeenstemming met het classificatieschema van de organisatie (zie hoofdstuk 3.1.8); zo nodig ook mapping tussen het eigen schema van de organisatie en het schema van de leverancier;
3. Wettelijke en regelgevende eisen, met inbegrip van gegevensbescherming, rechten van intellectueel eigendom en auteursrecht, en een beschrijving van hoe wordt gewaarborgd dat eraan wordt voldaan;
4. Verplichting van elke contractuele partij om een overeengekomen aantal beheersmaatregelen te implementeren, waaronder toegangsbeveiliging, prestatiebeoordeling, monitoren, rapporteren en auditen;
5. De regels van aanvaardbaar gebruik van informatie, met inbegrip van onaanvaardbaar gebruik indien noodzakelijk;
6. Hetzij een expliciete lijst van leverancierspersoneel dat geautoriseerde toegang heeft of bevoegd is informatie van de organisatie te ontvangen, hetzij procedures of voorwaarden voor autorisatie en het intrekken van de autorisatie, tot toegang tot of ontvangst van informatie van de organisatie door leverancierspersoneel;
7. Beleidsregels betreffende informatiebeveiliging die relevant zijn voor het specifieke contract;
8. Eisen voor incidentbeheer en -procedures (in het bijzonder notificatie en samenwerking tijdens herstel van het incident);
9. Trainings- en bewustzijnseisen voor specifieke procedures en informatiebeveiligingseisen, bijv. voor incidentresponsprocedures, autorisatieprocedures;
10. Relevante regelgeving voor onderaanneming, met inbegrip van de beheersmaatregelen die moeten worden geïmplementeerd;
11. Relevante overeenkomstpartners, met inbegrip van een contactpersoon voor aangelegenheden betreffende informatiebeveiliging;
12. Indien relevant, screeningseisen voor leverancierspersoneel, met inbegrip van verantwoordelijkheden voor het uitvoeren van de screening en notificatieprocedures indien de screening niet is voltooid of de resultaten aanleiding geven tot twijfel of bezorgdheid;
13. Het recht om de processen en beheersmaatregelen van de leverancier in verband met de overeenkomst te auditen;
14. Procedures voor het oplossen van defecten en conflicten;
15. Verplichting van de leverancier om periodiek een onafhankelijk rapport te verstrekken over de doeltreffendheid van beheersmaatregelen, en overeenkomst over tijdige correctie van relevante kwesties die in het rapport aan de orde worden gesteld;
16. Verplichting van de leverancier om te voldoen aan de beveiligingseisen van de organisatie.
 |
| **1.16** | **15.1.3** | Toeleveringsketen van informatie- en communicatietechnologie: Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico’s in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie. |
|  |  | **Tips:** in de bewerkersovereenkomst (privacy bijsluiter), als bijlage bij het contract, moet ook verwezen worden naar sub-bewerkers. Bovendien moet er periodiek een terugkoppeling gepresenteerd worden in een SLR (Service Level Rapportage) op tenminste de bedrijfskritische applicaties. Zie ook "Leidraad Informatiebeveiligingsbeleid XX-V2.0". |
| **1.17** | **16.1.1** | Verantwoordelijkheden en procedures: Er zijn leidinggevende en -procedures vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen. |
|  |  | **Tips:** zijn de taken die te maken hebben met informatiebeveiliging opgenomen in de functiebeschrijving van de leidinggevende. |
| **1.18** | **16.1.2** | Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. |
|  |  | **Tips:** er is een goede escalatieprocedure beschikbaar. |
| **1.19** | **18.1.3** | Beschermen van registraties: Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave. |
|  |  | **Tips:** hanteer het document met afgesproken bewaartermijnen binnen een instelling (**D**ocumentair **S**tructuur**p**lan - DSP). Dataportabiliteit is een voorwaarde. Fysieke documenten vallen buiten de scope. |
| **1.20** | **18.1.4** | Privacy en bescherming van persoonsgegevens: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. |
|  |  | **Tips:** privacy kan onderdeel zijn van het informatiebeveiligingsbeleid zoals opgenomen in hoofdstuk 3.1.1. |
| **1.21** | **6.1.2** | Scheiding van taken: Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. |
|  |  | **Tips:** scheiden van taken op basis van functies en rollen. Transparantie op het gebied van OTAP en autorisatiematrix. Waarborgen van functiescheiding. |

##  Personeel, studenten en gasten

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **2.1** | **7.1.2** | **Arbeidsvoorwaarden**: De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden. |
|  |  | **Tips:** geen aanvullende opmerkingen |
| **2.2** | **7.2.2** | **Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging:** Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. |
|  |  | **Tips:** geen aanvullende opmerkingen |
| **2.3** | **9.2.6** | **Toegangsrechten intrekken of aanpassen:** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast. |
|  |  | **Tips:** de autorisatiematrix is voor dit statement cruciaal. Met name de medewerkers die uit dienst zijn getreden moeten worden ge-audit. Het betreft hier medewerkers en externen die een nieuwe rol of functie krijgen (life cycle) en de medewerkers en externen die de instelling verlaten (de-provisioning). Studenten worden niet meegenomen, omdat zij geen groot risico vormen in het kader van informatiebeveiliging (zie Cyberdriegingsbeeld 2016).Zie ook hoofdstuk 3.5.1. |
| **2.4** | **11.2.9** | **‘Clear desk’- en ‘clear screen’-beleid**: Er behoort een ‘clear desk’-beleid voor papieren documenten en verwijderbare opslagmedia en een ‘clear screen’-beleid voor informatie verwerkende faciliteiten te worden ingesteld. |
|  |  | **Tips**: een audit kan ook plaatsvinden op afvalpapier. Het komt (kwam) vaak voor dat waardedocumenten in een afvalbak werden gegooid zonder dat informatie onleesbaar is (was) gemaakt. |
| **2.5** | **13.2.4** | **Vertrouwelijkheids- of geheimhoudingsovereenkomst:** Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd. |
|  |  | **Tips:** geheimhoudingsovereenkomst beoordelen. Onderzoek met name de deelnemersadministratie. T.a.v. de geheimhouding kan ook verwezen worden naar de cao. |
| **2.6** | **16.1.3** | **Rapportage van zwakke plekken in de informatiebeveiliging:** Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren. |
|  |  | **Tips:** werknemers moeten zwakke plekken melden. Een “Responsible Disclosure” beleid is dan wenselijk. Zie de SURF Beleidsnotitie Modelbeleid en procedure responsible disclosure.[[2]](#footnote-2) |
| **2.7** | **7.1.1** | **Screening**: Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico’s te zijn. |
|  |  | **Tips:** instelling moet een screeningsbeleid hebben waarvan de verklaring Omtrent Gedrag (VOG) een onderdeel is. Dit moet ook overlegd worden door tijdelijke externe medewerkers. In sommige sectoren (mbo, po, vo) is dit een verplichting. |

## Ruimtes en apparatuur

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **3.1** | **6.2.1.2** | **Beleid voor mobiele apparatuur:** Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico’s die het gebruik van mobiele apparatuur met zich meebrengt te beperken. |
|  |  | **Tips:** de apparatuur van de organisatie wordt geregistreerd; sommige instellingen registreren ook de eigen apparatuur (BYOD). Dit wordt beschreven in een beleidsdocument (bijv. de AUP). |
| **3.2** | **8.3.2** | **Verwijderen van media:** Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures. |
|  |  | **Tips:** geen aanvullende opmerkingen |
| **3.3** | **11.1.1** | **Fysieke beveiligingszone:** Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten. |
|  |  | **Tips:** gebruik van pasjes, die vervolgens gelogd worden. Maar ook een sleutelplan. De rechten van de huishoudelijke dienst kunnen als onderzoekvraag worden meegenomen. In scope zijn bijv. ICT-ruimten, archiefruimten, etc. |
| **3.4** | **11.1.2** | **Fysieke toegangsbeveiliging:** Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt. |
|  |  | **Tips:** plattegrond met zone classificatie. ICT-ruimten zijn alleen toegankelijk voor geautoriseerde medewerkers (geen conciërges, facilitaire beheerders en onderhoudspersoneel). |
| **3.5** | **11.1.3** | **Kantoren, ruimten en faciliteiten beveiligen:** Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast. |
|  |  | **Tips:** controle op examenruimten is wenselijk. Onderzoek ook de rechten van externen. Scope: Alleen ICT-ruimten of aan ICT gerelateerde ruimten. |
| **3.6** | **11.1.4** | **Beschermen tegen bedreigingen van buitenaf:** Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast. |
|  |  | **Tips:** beleid opnemen in 3.1.1. Kern is het inwinnen van specialistisch advies. BCM en (bijvoorbeeld) ARBO-specialisten. |
| **3.7** | **11.1.5** | **Werken in beveiligde gebieden:** Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast. |
|  |  | **Tips:** het betreft hier werken in MER, SER, serverruimten e.d. ARBO kan hier aanvullende informatie opleveren. |
| **3.8** | **11.1.6** | **Laad- en loslocatie:** Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden. |
|  |  | **Tips:** nieuwe notebooks kunnen gestolen worden of voorzien worden van ongewenste software. Denk ook aan terreurdreiging. |
| **3.9** | **11.2.1** | **Plaatsing en bescherming van apparatuur:** Apparatuur behoort zo te worden geplaatst en beschermd dat risico’s van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind. |
|  |  | **Tips:** aantal aandachtspunten: * Plaats waardevolle apparatuur niet in het zicht.
* Schroef desktops vast.

Blindeer ramen van ruimten waar computers staan indien die gelokaliseerd zijn aan de straatkant. |
| **3.10** | **11.2.2** | **Nutsvoorzieningen:** Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen. |
|  |  | **Tips:** beoordeel o.a. noodstroomvoorzieningen zoals aanwezigheid UPS (Uninterruptible Power Supply). Scope: vitale apparatuur. |
| **3.11** | **11.2.3** | **Beveiliging van bekabeling:** Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **3.12** | **11.2.4** | **Onderhoud van apparatuur:** Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen. |
|  |  | **Tips:** scope: IT-infrastructuur. Onderhoudscontracten (SLA en SLR) moeten op orde zijn. |
| **3.13** | **11.2.6** | **Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein:** Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico’s van werken buiten het terrein van de organisatie. |
|  |  | **Tips:** afspraken opnemen in AUP. |
| **3.14** | **11.2.7** | **Veilig verwijderen of hergebruiken van apparatuur:** Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven. |
|  |  | **Tips:** het betreft hier afvoer van apparatuur. |
| **3.15** | **12.4.4** | **Kloksynchronisatie:** De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron. |
|  |  | **Tips:** De systeemklokken van alle relevante infrastructuur componenten (zoals switches, servers, werkstations en appliances) dienen geautomatiseerd gesynchroniseerd te worden met een betrouwbare bron. In het beheerde netwerk moet een redundant uitgevoerde NTP[[3]](#footnote-3)-bron geplaatst te zijn waarmee elke infrastructuur component zijn systeemklok synchroniseert. Deze NTP-bron synchroniseert op zijn beurt met een geautoriseerde NTP-bron van het internet. |

## Continuïteit

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **4.1** | **12.1.2** | **Wijzigingsbeheer:** Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **4.2** | **12.1.4** | **Scheiding van ontwikkel-, test- en productieomgevingen** Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. |
|  |  | **Tips:** audit aanpassen aan SaaS applicaties. |
| **4.3** | **12.2.1.1** | **Beheersmaatregelen tegen malware:** Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd. |
|  |  | **Tips:** vragen die gesteld kunnen worden: “Doen we het?” en “Hoe doen we het?”. |
| **4.4** | **12.2.1.2** | **Beheersmaatregelen tegen malware:** Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten ten aanzien van het gevaar van virussen en dergelijke. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **4.5** | **12.3.1.1** | **Back-up van informatie:** Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt.  |
|  |  | **Tips:** controle van het back-up volume is gewenst (is van alle informatie een back-up gemaakt?). Controleer logboek back-up. |
| **4.6** | **12.3.1.2** | **Back-up van informatie:** Gemaakte back ups worden regelmatig getest conform het back-up beleid. |
|  |  | **Tips:** terugzetten van bestanden (restore) middels een logboek controleren. |
| **4.7** | **12.5.1** | **Software installeren op operationele systemen:** Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd. |
|  |  | **Tips:** toevoegen aan niveau 3: zowel de beheerder als de **gebruiker** moet de procedures kunnen vinden. De doelstelling is generiek, dus bijv. laptops vallen er ook onder.  |
| **4.8** | **12.6.1** | **Beheer van technische kwetsbaarheden:** Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken. |
|  |  | **Tips:** Worden de updates van (bijvoorbeeld) Microsoft (hot fixes) uitgevoerd. Wordt er periodiek een pentest uitgevoerd. Denk ook aan hardening van servers. Wordt er periodiek getest op kwetsbaarheden en worden ernstige kwetsbaarheden vervolgens opgelost. |
| **4.9** | **12.6.2** | **Beperkingen voor het installeren van software:** Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **4.10** | **14.2.6** | **Beveiligde ontwikkelomgeving:** Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling. |
|  |  | **Tips:** beoordeling SaaS omgeving is eenvoudiger. Bij SaaS focus op acceptatie omgeving. Deze leidt tot de beoordeling van de evidence, met name op basis van aangeleverde certificering van leverancier. |
| **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. |
|  |  | **Tips:** basis zijn gesprekken met leveranciers betreffende SLA’s en SLR’s. Informatie van leverancier is daarbij leidend. |
| **4.12** | **16.1.4** | **Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen:** Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiliging incidenten. |
|  |  | **Tips:** geen aanvullende opmerkingen. Een beveiligingsincident kan leiden tot een datalek, dit is niet altijd het geval (bijvoorbeeld, gestolen notebook is versleuteld). Classificatieflow datalekken. |

|  |  |  |
| --- | --- | --- |
| **4.13** | **16.1.5** | **Respons op informatiebeveiligingsincidenten:** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **4.14** | **17.1.2** | **Informatiebeveiligingscontinuïteit implementeren:** De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen. |
|  |  | **Tips:** Continuïteit van de beveiliging van informatievoorziening. |
| **4.15** | **17.2.1** | **Beschikbaarheid van informatie verwerkende faciliteiten:** Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen. |
|  |  | **Tips:** betrek hier ook de keten bij. |

## Toegangsbeveiliging en integriteit

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **5.1** | **9.1.1** | **Beleid voor toegangsbeveiliging:** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. |
|  |  | **Tips:** toegangsbeveiliging zowel voor het netwerk als voor applicaties. Zie “Leidraad toegangsbeveiliging”. |
| **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. |
|  |  | **Tips:** het betreft hier technische netwerkdiensten, denk aan VPN en draadloos netwerk. |
| **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. |
|  |  | **Tips:** het betreft nieuwe gebruikers en het verwijderen van gebruikers. |
| **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. |
|  |  | **Tips:** het verlenen van toegangsrechten tot applicaties op basis van functie en rollen (RBAC) van medewerkers. |
| **5.5** | **9.2.3** | **Beheren van speciale toegangsrechten:** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst. |
|  |  | **Tips:** het betreft hier de super users / administrators rechten. |
| **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. |
|  |  | **Tips:** het betreft het wachtwoordenbeleid dat op basis van delegatie is goedgekeurd. |
| **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. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **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. |
|  |  | **Tips:** de gebruiker ziet alleen die opties in het keuzemenu waartoe hij rechten heeft. |
| **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. |
|  |  | **Tips:** een aantal aanbevelingen:* 2-way authenticatie;
* Wachtwoord kan niet worden “afgeluisterd”;
* Wachtwoord wordt niet weergegeven;

Wachtwoord en username komen niet overeen is de juiste foutmelding bij onjuist ingetypt wachtwoord. |
| **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. |
|  |  | **Tips:** beleid t.a.v. digitale sleutels. Bijvoorbeeld wanneer Bitlocker wordt toegepast is er een beleid waarin wordt omschreven hoe de sleutel wordt beheerd, hoe versleutelde bestanden teruggehaald kunnen worden bij verlies van de originele encryptiesleutel en hoe vervolgens een nieuwe encryptiesleutel wordt ingevoerd. |
| **5.11** | **10.1.2.2** | **Sleutelbeheer:** Er wordt gebruik gemaakt van tools om cryptografische sleutels tijdens hun gehele levenscyclus adequaat te beheren. |
|  |  | **Tips:** beheer van cryptografische sleutels (bijvoorbeeld Bitlocker maakt ook gebruik van een cryptografische sleutel). |
| **5.12** | **12.4.2** | **Beschermen van informatie in logbestanden:** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **5.13** | **13.1.1** | **Beheersmaatregelen voor netwerken:** Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen. |
|  |  | **Tips:** beoordeling netwerk security. De volwassenheid van de documentatie van het netwerk wordt beoordeeld. |
| **5.14** | **13.1.2** | **Beveiliging van netwerkdiensten:** Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **5.15** | **13.1.3** | **Scheiding in netwerken:** Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden. |
|  |  | **Tips:** zie “Leidraad toegangsbeveiliging” (cf. 3.5.1) |
| **5.16** | **13.2.3** | **Elektronische berichten**: Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd |
|  |  | **Tips:** toetsen op certificering. Zie ook 3.1.12. |
| **5.17** | **14.1.3** | **Transacties van toepassingen beschermen:** Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen. |
|  |  | **Tips:** Toetsen op vertrouwelijkheid, SSL-certificaat, officieel certificaat. Maar ook toetsen op integriteit. Bijvoorbeeld de koppeling naar DUO op basis van certificaten uitgegeven door een valide CA (bijv. SURFcertificaten-Digicert). |

## Controle en logging

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **6.1** | **9.2.5** | **Beoordeling van toegangsrechten van gebruikers:** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. |
|  |  | **Tips:** een van de belangrijkste statements. De proceseigenaar moet samen met hoofd systeembeheer controleren of de toegangsrechten juist zijn. De accountant controleert dit statement regelmatig. Zie ook “Leidraad toegangsbeveiliging” (cf. 3.5.1). |
| **6.2** | **12.4.1** | **Gebeurtenissen registreren:** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **6.3** | **12.4.3** | **Logbestanden van beheerders en operators:** Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **6.4** | **14.2.7** | **Uitbestede softwareontwikkeling:** Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **6.5** | **14.2.8** | **Testen van systeembeveiliging:** Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **6.6** | **14.2.9** | **Systeemacceptatietests:** Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma’s voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **6.7** | **15.2.1** | **Monitoring en beoordeling van dienstverlening van leveranciers:** Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen. |
|  |  | **Tips:** geen aanvullende opmerkingen. |
| **6.8** | **16.1.7** | **Verzamelen van bewijsmateriaal:** De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen. |
|  |  | **Tips:** bewijs dat gebruikt kan worden in een rechtszitting. Zodra een juridische procedure dreigt is het verstandig externe expertise in te huren om het maken van procedurefouten te voorkomen. |
| **6.9** | **18.2.2** | **Naleving van beveiligingsbeleid en –normen:** Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging. |
|  |  | **Tips:** proceseigenaren controleren of afspraken gerealiseerd zijn. Vragen zijn in de trant van: “Waar liggen de verantwoordelijkheden?” zijn beantwoord en gedocumenteerd. |
| **6.10** | **18.2.3** | **Beoordeling van technische naleving:** Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging. |
|  |  | **Tips:** beoordeling op technisch inhoudelijk gebied. |

# Compliance-kader privacy

Privacywetgeving vanuit de overheid is ook voor het mbo van toepassing is. In deze wet- en regelgeving zijn zowel informatiebeveiligingsaspecten als specifieke privacyaspecten opgenomen. Samen met SURF en Kennisnet is van al deze aspecten een set van statements gemaakt.

Veel van de vereiste informatiebeveiligingsaspecten komen terug in de statements van het normenkader informatiebeveiliging mbo, dat gebaseerd is op ISO 27002. Het kan dan ook gezegd worden dat allereerst de generieke informatiebeveiliging op orde moet zijn.

Maar voor het handhaven van de privacy is er echter een aantal statements dat meer aandacht nodig heeft of is er reden om nadere invulling van bestaande statements te overwegen. Hieruit volgt een set van **38** gemeenschappelijke statements voor informatiebeveiliging en privacy. In dit document staat bij die statements een toelichting over de relatie met privacy. Waar bij het algemene toetsingskader informatiebeveiliging wellicht een niveau 2 voldoende is, is het in het kader van de privacy van belang om hier naar een hoger ambitieniveau te streven, bijvoorbeeld een niveau 3 of zelfs 4.

Naast deze gemeenschappelijke statements is er ook behoefte aan een aanvullende set van statements om volledig aan de eisen uit de betreffende wet- en regelgeving te voldoen. Daarom is een compleet compliance-kader privacy voor het mbo onderwijs opgesteld. Dit compliance-kader bestaat uit **24** specifieke privacy statements die zijn opgenomen in een apart document: IBPDOC2b compliance kader privacy voor het mbo. Dit is een juridisch normenkader, dat nader is uitgewerkt in het toetsingskader privacy conform de MBOaudit werkwijze.

## Basis privacy principes

### Privacy by design[[4]](#footnote-4)

Privacy is uitgangspunt: *privacy by design* (de AVG spreekt overigens over ‘gegevensbescherming door ontwerp). Zonder het respecteren en erkennen van elkaar privacy, is privacy niet mogelijk. Het respecteren van privacy is uitgangspunt en staat niet ter discussie. Privacybescherming is alleen mogelijk als we daar afspraken (regels) voor maken en nakomen. Voor iedereen moeten de zelfde uitgangspunten gelden. Uitvoering van alle hier opvolgende principes ligt in het verlengde van het respect voor de zorgvuldige omgang met en bescherming van persoonsgegevens in overeenstemming met de wet. Dat betekent dat omgang met persoonsgegevens is gebaseerd op rechtmatig, eerlijk en transparant handelen ten opzichte van de betrokkene. Rechtmatigheid (grondslag) en transparantie worden in eigen beginselen uitgewerkt, en met eerlijkheid wordt een behoorlijke en fatsoenlijke omgang met betrokkenen en hun belangen gewaarborgd. Door bij ieder gebruik van persoonsgegevens vooraf na te denken over het doel van dat gebruik, wordt bereikt dat privacybescherming standaard wordt en niet een sluitpost is.

### Doel en doelbinding

Iedereen moet zelf kunnen beschikken en beslissen over zijn eigen persoonsgegevens. Daarom mogen persoonsgegevens niet zomaar verzameld worden. Het moet duidelijk zijn waarvoor deze worden gebruikt. Dit doel wordt vastgesteld voordat de informatie wordt verzameld. Het gebruik van de persoonsgegevens moet overeenkomen met het doel, en mag daar niet mee onverenigbaar zijn. De gegevens zijn exclusief beschikbaar voor alleen dit vooraf bepaalde doel. Dit betekent dat deze gegevens - behoudens toestemming van betrokkene of op grond van de wet - niet bekend mogen worden gemaakt, beschikbaar gesteld of anderszins gebruikt voor andere doeleinden dan die vooraf zijn overeengekomen. Verstrekking aan anderen (derden), kan bijvoorbeeld alleen als dat nodig is om het doel te bereiken.

### Grondslag

Persoonsgegevens kunnen alleen op basis van een rechtmatig (wettelijk bepaald) doel worden verwerkt. Persoonsgegevens moeten rechtmatig verkregen worden: hoe kom ik aan deze gegevens? Daarvoor is een grond nodig voor het gebruik van persoonsgegevens. Het universele uitgangspunt is dat de betrokkene toestemming geeft. Als dat niet mogelijk is, moet de wet een grondslag geven. In wetgeving, bijvoorbeeld de Wet bescherming persoonsgegevens, zijn de volgende gronden (grondslagen) toegestaan:

* toestemming: er is toestemming van de betrokkene;
* wettelijke verplichting: de verwerking van persoonsgegevens is wettelijk verplicht of opgedragen door de wetgever;
* publiekrechtelijke taak: voor de uitvoering van een publieke taak (overheid) is de verwerking van persoonsgegevens noodzakelijk;
* vitaal belang (bescherming van de betrokkene): het verwerken van persoonsgegevens is noodzakelijk om een ernstige bedreiging van de gezondheid van betrokkene beperken/voorkomen;
* gerechtvaardigd belang (belangenafweging): de gegevensverwerking is noodzakelijk waarbij het belang van het verwerken van die gegevens zwaarder weegt dan het privacy-belang van de betrokkene.

### Dataminimalisatie

Er zijn grenzen aan het verzamelen van persoonsgegevens. Informatie moet door wettige en eerlijke middelen en manieren zijn verkregen. Daarbij is de gegevensverzameling:

1. **proportioneel**: het verzamelen van persoonsgegevens moet redelijk zijn, het moet in verhouding staan tot het doel dat je wilt bereiken. De inbreuk op de privacy moet te rechtvaardigen zijn om je doel te bereiken.
2. **subsidiair**: het doel waarvoor de persoonsgegevens worden verzameld, wordt in redelijkheid niet op een andere manier bereikt dan door de persoonsgegevens te gebruiken. Er mogen geen alternatieven zijn die minder ingrijpend zijn voor de privacy van de betrokkene. Als gebruik van anonieme gegevens mogelijk is, mogen er geen persoonsgegevens worden gebruikt.

Proportionaliteit legt daarmee een bovengrens, terwijl subsidiariteit een zekere ondergrens stelt aan de aard en hoeveelheid uit te wisselen gegevens.

Persoonsgegevens worden alleen bewaard zolang het gestelde doeleinde nog niet is behaald, daarna worden ze verwijderd of vernietigd. Dit gaat over de (wettelijk bepaalde) bewaartermijnen.

### Transparantie

Omdat het gaat om persoonsgegevens van en over de betrokkene, moet deze volstrekt helder en begrijpelijk zijn geïnformeerd over welke gegevens er worden verzameld, en wat er met de gegevens gebeurt. Openheid en transparantie over de gegevensverwerking is het uitgangspunt. Bij voorkeur is er organisatie breed beleid ontwikkeld hoe er met persoonsgegevens wordt omgegaan, wat de doelen zijn, en wat de rechten en plichten zijn. Het is ook duidelijk hoe lang de gegevens worden bewaard, en met wie de gegevens zijn/worden gedeeld. Voorbeelden van transparantie zijn het privacyreglement (in de studiegids, op de website), of uitleg bij het aanmeld- en inschrijfformulier, hoe de onderwijsinstelling omgaat met de persoonsgegevens.

### Rechten van de betrokkene

In geval van verzameling van persoonsgegevens, heeft de betrokkene altijd, bij iedere stap, een aantal rechten.

Deze rechten moeten zonder belemmering kunnen worden uitgevoerd. Het gaat hierbij om de volgende rechten:

* De betrokkene wordt (vooraf) in begrijpelijke taal actief en laagdrempelig geïnformeerd over de gegevensverwerking.
* Op verzoek van de betrokkene wordt inzage geven welke persoonsgegevens er worden verwerkt.
* Op verzoek van de betrokkene worden ontbrekende of verkeerd vastgelegde persoonsgegevens gecorrigeerd.
* Op verzoek van de betrokkene worden persoonsgegevens die niet (langer) nodig zijn om de vastgestelde doelen te behalen verwijderd.
* De betrokkene kan verzet instellen tegen een verwerking van zijn persoonsgegevens die plaats vond op grond van een gerechtvaardigd belang. Een voorbeeld hiervan is het gebruik van persoonsgegevens door de leverancier van leermiddelen van de student. De student wil niet langer aanbiedingen krijgen en meldt zich af.

Deze rechten moeten binnen een redelijke tijd worden uitgeoefend, zonder dat de betrokkene een buitensporige vergoeding hoeft te betalen. De verstrekte informatie moet gemakkelijk verstaanbaar en begrijpelijk zijn.

Een voorbeeld voor de uitoefening van de rechten, is een student wiens ouders recent zijn gescheiden. Die student wil zien welke informatie over hem en zijn ouders is geregistreerd en vraagt om correctie van zijn gegevens.

### Bev**e**iliging

Er moet zorgvuldig worden omgegaan met de persoonsgegevens die iemand worden toevertrouwd: het gaat om andermans gegevens. Persoonsgegevens moeten zijn beschermd met een redelijke zekerheid en waarborgen tegen risico's zoals verlies of onbevoegde toegang, vernietiging, gebruik, wijziging of openbaarmaking van gegevens. Hierbij wordt voldaan aan algemeen geaccepteerde organisatorische en technische beveiligingsnormen, zoals ISO-normen.

### Datakwaliteit (data-integriteit)

Bij persoonsgegevens gaat het om informatie waarmee personen worden geïdentificeerd, gegevens die iets zeggen over een persoon. Daarom moet die informatie gegarandeerd juist, nauwkeurig, volledig en up-to-date zijn en blijven.

### Verantwoordelijkheid (responsibility)

Degene die de persoonsgegevens verzamelt (de ‘verantwoordelijke’), is verantwoordelijk voor de nakoming van deze algemene privacy regels en is daarop aanspreekbaar. De verantwoordelijke legt daarover verantwoording af. Ook als er anderen namens de verantwoordelijke met de persoonsgegevens willen werken, moet de verantwoordelijke met die partij (de ‘bewerker’) afspraken maken over deze algemene privacy regels. Verwerking vindt dus alleen plaats in overeenstemming met de wet. De verantwoordelijke draagt ook de bewijslast om dit aan te tonen. Ook speelt de verantwoordelijke een belangrijke rol bij verstrekking van gegevens aan derden. Bij vertrekking van gegevens aan een bewerker moeten er dan ook goede afspraken worden gemaakt.

### Eigendom

Privacy zegt iets over hoe moet worden omgegaan met persoonsgegevens. Daarbij is het niet relevant van wie die gegevens zijn. Dat is juist ook de kracht van privacy, ongeacht wáár de persoonlijke informatie staat, of van wie die is, er moet altijd zorgvuldig mee worden omgegaan.

Bij privacy gaat het om rechten en plichten van degenen die met die gegevens om moeten gaan. Daarbij kan iedereen een aparte rol hebben (verantwoordelijke, bewerker). Privacy maakt duidelijk wie bevoegd is om informatie te verstrekken aan andere partijen.

## Statements compliance-kader privacy

### Beleid en organisatie

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Statement** | **Principe** |
| **P.1** | **Privacy-beleid**: Ten behoeve van het garanderen van privacy van deelnemers en medewerkers en om te voldoen aan de relevante wet- en regelgeving, behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur. In dit beleid is voorzien in procedures voor het uitoefenen van de rechten van deelnemers en docenten. | 5) Transparantie |
| **P.2** | **Functionaris gegevensbescherming:** De instelling benoemt een functionaris voor de gegevensbescherming (FG), of indien dit niet mogelijk of wenselijk is een privacy officer (PO), die is belast met intern toezicht op de verwerkingen van persoonsgegevens binnen de instelling, en alle verwerkingen van persoonsgegevens inventariseert en registreert. De verantwoordelijke zorgt er voor dat alle andere beroepswerkzaamheden van de FG verenigbaar zijn met zijn taken en verplichtingen als FG en dat die niet tot een belangenconflict leiden. | 9) Verantwoordelijkheid |
| **P.3** | **Doelbepaling, doelbinding, grondslag, grond bij minderjarigen en dataminimalisatie.**De instelling draagt er zorg voor dat de volgende zaken zijn vastgesteld:**P.3a Doelbepaling:** De instelling draagt er zorg voor dat voor iedere categorie van verwerkingen – voorafgaand aan die verwerking - een specifiek doeleinde is vastgesteld, en dat dit doeleinde is gecommuniceerd bij de gegevensverzameling.**P.3b Doelbinding:** De instelling zorgt er voor dat persoonsgegevens alleen worden verwerkt voor het doeleinde waarvoor die gegevens verkregen zijn.**P.3c Grondslag (rechtmatigheid):** De instelling zorgt er voor dat persoonsgegevens altijd op basis van een wettelijke grondslag worden verwerkt. Daarbij maakt de instelling geen gebruik van opt-out regelingen als het gaat om verwerkingen van persoonsgegevens.**P.3d Grond bij minderjarigen:** Indien toestemming noodzakelijk is bij verwerkingen van persoonsgegevens van deelnemers jonger dan 16 jaar, dan wordt toestemming altijd afgestemd met de wettelijke vertegenwoordigers, en deze toestemming wordt vastgelegd en is reproduceerbaar. **P.3e Dataminimalisatie:** Het verwerken van persoonsgegevens moet redelijk zijn en in verhouding staan tot het te realiseren doel van die verwerking: de inbreuk op de privacy moet te rechtvaardigen zijn om het doeleinde te bereiken (proportionaliteit), de te verzamelen persoonsgegevens blijven beperkt tot datgene wat minimaal nodig is om de doeleinde(n) te bereiken waarvoor de data worden verwerkt (subsidiariteit). | 2) Doel en doelbinding3) Grondslag4) Dataminimalisatie  |
| **P.4** | **Registratieplicht:** Een verwerking van persoonsgegevens wordt gemeld aan de aangestelde Functionaris Gegevensbescherming die daartoe een (openbaar) register bijhoudt. | 9) Verantwoordelijkheid |
| **P.5** | **Bewaartermijnen:** Er is een actief archief- en vernietigingsbeleid: persoonsgegevens worden niet langer bewaard dan nodig voor het gestelde doeleinde. De instelling stelt op basis van de Archiefwet de vernietigings- en bewaartermijnen vast van de verwerkte persoonsgegevens. De instelling is in staat om *alle* persoonsgegevens die niet onder een wettelijke bewaartermijn vallen, op een eerste verzoek van de deelnemer (of als deze jonger is dan 16 jaar: diens ouders) te vernietigen. | 4) Dataminimalisatie  |

|  |  |  |
| --- | --- | --- |
| **P.6** | **Verwerking t.b.v. onderzoek:** Persoonsgegevens mogen worden verwerkt ten behoeve van: 1. archivering in het algemeen belang (Archiefwet);
2. wetenschappelijk of historisch onderzoek of
3. statistische doeleinden.

Indien passende technische en organisatorische maatregelen zijn genomen om de privacy van de betrokken deelnemers te garanderen. Onder deze maatregelen wordt in ieder geval verstaan dat er niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk is. Hierbij valt te denken aan pseudonimisering (in geval de data herleidbaar moet zijn tot individuen) of anonimisering (in geval data niet herleidbaar hoeft te zijn). Bij historische, statistische of wetenschappelijke doeleinden is verwerking alleen mogelijk op basis van strikte voorwaarden vergelijkbaar met de ‘Gedagscode voor Onderzoek & Statistiek’ en de verantwoordelijke voorafgaand toestemming heeft verleend.  | 2) Doel en doelbinding |
| **P.7** | **Verwerking van bijzondere persoonsgegevens:**De instelling verwerkt geen persoonsgegevens betreffende * iemands religieuze of levensbeschouwelijke overtuigingen, tenzij dit gelet op het doel van de instelling en voor de verwezenlijking van haar grondslag strikt noodzakelijk is,
* ras of etnische afkomst, tenzij de instelling daartoe op grond van een wet verplicht is, of alleen in met het doel om personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen om feitelijke nadelen verband houdende met de grond ras op te heffen of te verminderen,
* biometrische gegevens (zoals vingerafdruk of irisscan) met het oog op de unieke identificatie van een persoon,
* gezondheid of iemands seksueel gedrag of seksuele gerichtheid, voor zover dat met het oog op de speciale begeleiding van deelnemers of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is,

tenzij de deelnemer voor het gebruik van deze categorieën persoonsgegevens zelf toestemming heeft gegeven voor het verwerken van de hiervoor genoemde categorieën persoonsgegevens voor een welbepaald doel.  | 2) Dataminimalisatie |
| **P.8** | **Geautomatiseerde besluitvorming:** In geval de instelling gebruik maakt van geautomatiseerde individuele besluitvorming:* zal de onderwijsinstelling geen geautomatiseerde beslissingen laten nemen over de betrokkene zonder dat bij die beslissing een natuurlijk persoon namens de instelling betrokken is, tenzij de betrokkene instemt met een geautomatiseerde beslissing zonder menselijke interventie; en
* zal er aan de betrokkene duidelijke informatie worden verstrekt over de wijze van profilering, en
* heeft de betrokkene de mogelijkheid
	+ zijn standpunt en visie over het besluit en besluitvormingsproces te geven, en
	+ in verweer te komen tegen een dergelijke geautomatiseerde beslissing;
* worden er bij de besluitvorming geen bijzondere persoonsgegevens gebruikt.
 | 2) Doel en doelbinding |

|  |  |  |
| --- | --- | --- |
| **P.9** | **Informatiebeveiliging**: De instelling neemt passende technische of organisatorische maatregelen op een dusdanige manier dat de passende beveiliging van persoonsgegevens gewaarborgd is. De integriteit en vertrouwelijkheid van de persoonsgegevens moet gegarandeerd zijn. Verwerkte persoonsgegevens zijn beveiligd tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze beveiliging is afhankelijk van de stand van de techniek, de uitvoeringskosten, alsook de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de privacy van de onderwijsdeelnemers. Bij de beveiliging wordt aangesloten bij algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging. | 7) Beveiliging |
| **P.10** | **Bewerkersovereenkomsten**: Met alle leveranciers die als bewerker voor of namens de instelling persoonsgegevens (van deelnemers, medewerkers en externen) verwerken, worden bewerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld. | 9) Verantwoordelijkheid |

### Personeel, studenten en gasten

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Statement** | **Principe** |
| **P.11** | **Transparantie privacy beleid:** De instelling informeert de (ouders van) deelnemers en medewerkers van wie persoonsgegevens worden verwerkt, beknopt, transparant, eenvoudig toegankelijk en begrijpelijk in duidelijke en eenvoudige taal over het privacy beleid en de rechten en verplichtingen van betrokkenen. | 5) Transparantie |
| **P.12** | **Informatieplicht verwerkingen:** De instelling informeert actief, al dan niet met gebruikmaking van door leveranciers geleverde informatie, aan de (ouders van) deelnemers en medewerkers van wie persoonsgegevens worden verwerkt, welke verwerking er in welke informatiesystemen binnen de instelling plaatsvindt en welke maatregelen er zijn getroffen om de privacy van die deelnemer te kunnen waarborgen.Aan de betrokken deelnemers en docenten wordt beknopt, transparant, eenvoudig toegankelijk en begrijpelijk in duidelijke en eenvoudige taal ten minste medegedeeld: * De identiteit en contactgegevens van de verantwoordelijke (CvB van de onderwijsinstelling),
* De contactgegevens van de FG of PO,
* welke (categorieën) persoonsgegevens worden verwerkt,
* het doel van de verwerking,
* of die verwerking beperkt is tot dat wat voor het gestelde doeleinde strikt noodzakelijk is,
* of persoonsgegevens ook voor andere doeleinden worden verwerkt,
* wat de bewaar- en vernietigingstermijnen zijn;
* of persoonsgegevens worden gedeeld met commerciële derden,
* of persoonsgegevens worden verkocht of verhuurd,
* of persoonsgegevens gecodeerd worden bewaard.
 | 5) Transparantie |
| **P.13** | **Rechten van betrokkene:** De instelling respecteert expliciet de volgende rechten:**P.13.a.** Deelnemers (dan wel hun ouders) en medewerkers hebben het recht een verzoek te doen ter verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens, in het geval dat deze gegevens: * + feitelijk onjuist zijn,
	+ voor het gestelde doeleinde onvolledig of niet ter zake dienend zijn,
	+ de verwerking van de persoonsgegevens niet meer nodig is,
	+ dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt.

**P.13.b.** De verbetering, aanvulling of verwijdering wordt voor zover redelijkerwijs mogelijk doorgegeven aan alle personen en organisaties die van de onderwijsinstelling hebben ontvangen. **P.13.c.** Deelnemers hebben het recht om geheel ‘te worden vergeten’ door het verwijderen van alle persoonsgegevens, tenzij de onderwijsinstelling op grond van een wettelijke plicht, of ter vrijwaring van een rechtsvordering deze gegevens moet bewaren. Evenmin worden de gegevens verwijderd indien deze verwijdering een inbreuk op vrijheid van meningsuiting en informatie oplevert. **P.13.d.** In geval de verwerking van persoonsgegevens plaatsvindt op basis van toestemming of een overeenkomst, heeft de deelnemer heeft recht om de door de onderwijsinstelling verwerkte persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen. **P.13.e.** De betrokken deelnemer wordt in kennis gesteld van de door de onderwijsinstelling uitgevoerde handelingen met zijn persoonsgegevens. | 6) Rechten betrokkene |
| **P.14** | **Arbeidsvoorwaarden**: In de contractuele overeenkomst met medewerkers en contractanten zijn hun (eventuele) verantwoordelijkheden voor privacy opgenomen. In deze overeenkomst is voorzien in een vertrouwelijkheids- of geheimhoudingsbeding ten aanzien van de verwerkte persoonsgegevens. | 9) Verantwoordelijkheid |
| **P.15** | **Bewustzijn, opleiding en training ten aanzien van privacy:** Alle interne en externe medewerkers van de organisatie behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. De FG is hierbij betrokken. | 5) Transparantie |

### Ruimtes en apparatuur

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Statement** | **Principe** |
| **P.16** | **Verwijderen van persoonsgegevens:**van apparatuur die niet langer wordt gebruikt, worden de op het apparaat aanwezige persoonsgegevens op een betrouwbare en veilige wijze vernietigd. Vernietiging is mogelijk door vernietiging van de gegevensdrager zelf. In geval van vernietiging door een derde, geeft deze een verklaring af aangaande vernietiging. | 4) Dataminimalisatie7) Beveiliging |

### Vertrouwelijkheid en integriteit

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Statement** | **Principe** |
| **P.17** | **Datakwaliteit (data-integriteit):** De verantwoordelijke gaat zorgvuldig om met de verwerkte persoonsgegevens en waarborgt het behoud en bescherming van de juistheid en de consistentie van die gegevens. | 8) Datakwaliteit |
| **P.18** | **Datalek:** In geval van een inbreuk in verband met de (beveiliging van) persoonsgegevens die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.En die inbreuk houdt een risico in voor de rechten en vrijheden van betrokkenen, dan meldt de verantwoordelijke de inbreuk bij de AP zo snel mogelijk, doch uiterlijk binnen 72 uur nadat de inbreuk bekend is geworden. Deze inbreuk wordt aan getroffen betrokkenen gemeld indien de inbreuk een waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen. De getroffen deelnemers en medewerkers worden geïnformeerd over de aard van de inbreuk, en de gevolgen van de inbreuk op hun privacy. | 5) Transparantie |
| **P.19** | **Bijzondere persoonsgegevens:** Bij verwerking van bijzondere persoonsgegevens zoals gezondheidsgegevens, neemt de instelling (extra) passende, consequente en specifieke maatregelen om de veiligheid van de gegevens te garanderen. Het gebruik van deze bijzondere gegevens blijft beperkt tot alleen die gevallen dat de informatie strikt noodzakelijk en evenredig is. | 4) Beveiliging |

### Controle en logging

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Statement** | **Principe** |
| **P.20** | **Privacy in informatiesystemen**: Bij het gebruiken en/of ontwerpen van informatiesystemen die persoonsgegevens van deelnemers en medewerkers verwerken, worden privacyregels zoals privacy by design en privacy by default in die systemen een aangehouden en zo mogelijk ingebouwd: • Gegevensminimalisatie af te dwingen (zo min mogelijk vrije velden)• Transparantie over gebruik van gegevens• Afschermen van de identiteit (pseudonimisering)• Gebruik sticky policies* Data tracking (waaronder logging).
 | 4) Dataminimalisatie8) Datakwaliteit |
| **P.21** | **Gegevensbeschermingseffectbeoordeling (GEB, voorheen PIA):** * De instelling voert een (tweejaarlijks terugkerende) evaluatie uit van de mogelijke effecten van de verschillende gegevensverwerking op de rechten en vrijheden van de betrokkenen. Deze evaluatie vindt eveneens plaats in geval van een wijziging in de verwerking van persoonsgegevens die specifiek de risico’s wijzigt voor de privacy van de betrokken deelnemers en medewerkers.
* De instelling voert naar aanleiding van de evaluatie een volledige GEB uit in geval de verwerking van de persoonsgegevens:
	+ in geval van een systematische en uitgebreide beoordeling van persoonlijke aspecten van betroknnen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
	+ Bijzondere persoonsgegevens (ras, gezondheid) worden verwerkt;
	+ Geautomatiseerde bewaking van publiek toegankelijke ruimtes.
* De beoordeling heeft betrekking op de gehele levenscyclus van persoonsgegevens van verzameling van verwerking tot verwijdering.
* In geval van herziening van of nieuwe verwerkingen van grote hoeveelheden persoonsgegevens, wordt vooraf bepaald wat de impact is van deze (gewijzigde) verwerking op de privacy van de deelnemers.

Bij de GEB is altijd de FG betrokken. | 2) Doel en doelbinding7) Doel en doelbinding8) Datakwaliteit |
| **P.22** | **Naleving van privacy beleid en –normen:** De instelling controleert (laat controleren) regelmatig de naleving van de privacy regels en informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging. De FG ziet toe op de (dagelijkse) naleving van het beleid. | 9) Verantwoordelijkheid |
| **P.23** | **Rapportage van privacy-gebeurtenissen**: Privacy- en informatiebeveiligingsincidenten behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd aan de FG en verantwoordelijke. | 7) Beveiliging |
| **P.24** | **Gebeurtenissen registreren:** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzoneringen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig beoordeeld. | 5) Transparantie 9) Verantwoordelijkheid |

## Statements gemeenschappelijk normenkader

### Cluster 1: Beleid en organisatie

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **1.1** | **5.1.1.1** | **Beleidsregels voor informatiebeveiliging**: Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur |
| **Privacy toets:** Hanteer als uitgangspunt IBPDOC6 Model informatiebeveiliging en privacy beleid voor de mbo sector. Indien gebruik wordt gemaakt van een eigen beleidsplan controleer dan de volgende onderdelen op aanwezigheid en juistheid:1. Inleiding 2. Beleidsuitgangspunten en -principes informatiebeveiliging en privacy 3. Classificatie4. Wet- en regelgeving5. Governance informatiebeveiligingsbeleid6. Melding en afhandeling van incidenten |
| **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. |
| **Privacy toets:** onderzoek of er ook met externe partijen wordt gecommuniceerd over het informatiebeveiliging en privacy beleid van de mbo instelling. |
| **1.6** | **6.2.1.1** | **Beleid voor mobiele apparatuur**: Er dient beleid te worden vastgesteld om de risico’s die het gebruik van mobiele apparatuur met zich meebrengt te beheren. |
| **Privacy toets:** er is een beleid op het gebied van Bring Your Own Device (BYOD) en Bring Your Company Device (BYCD). Bovendien wordt dit beleid gecontroleerd. |
| **1.7** | **8.2.1** | **Classificatie van informatie**: Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging. |
| **Privacy toets:** 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. Deze classificatie wordt gebruikt en periodiek geëvalueerd. |
| **1.8** | **8.2.2** | **Informatie labelen**: Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie. |
| **Privacy toets:** de mbo instelling moet kunnen aantonen dat de classificatie daadwerkelijk wordt toegepast. Te denken valt aan:* Security architectuur document;
* Documenten die voorzien zijn van een ‘stempel’ vertrouwelijk;
* Aanwezigheid van een vertrouwenspersoon;
* Aanvullende afspraken voor functioneel beheerders i.v.m. vertrouwelijkheid;

Etc. |
| **1.9** | **10.1.1.1** | **Beleid inzake het gebruik van crypto grafische beheersmaatregelen:** Ter bescherming van informatie behoort een beleid voor het gebruik van crypto grafische beheersmaatregelen te worden ontwikkeld. |
| **Privacy toets:** Er is een beleid t.a.v. crypto grafische beheersmaatregelen. |
| **1.10** | **10.1.1.2** | **Beleid inzake het gebruik van crypto grafische beheersmaatregelen**: Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van crypto grafische beheersmaatregelen wordt geïmplementeerd. |
| **Privacy toets:** de mbo instelling heeft een of meerder tools aangeschaft ihkv crypto grafische beheersmaatregelen. |
| **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. |
| **Privacy toets:** eisen worden opgenomen in SLA’s en (bijvoorbeeld) maandelijks teruggekoppeld in een SLR (Service Level Rapportage). |
| **1.18** | **16.1.2** | **Rapportage van informatiebeveiligingsgebeurtenissen:** Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. |
| **Privacy toets:** er is een goede escalatie procedure beschikbaar. |
| **1.19** | **18.1.3** | **Beschermen van registraties**: Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave. |
| **Privacy toets:** er is een document met afgesproken bewaartermijnen binnen een mbo instelling. |
| **1.20** | **18.1.4** | **Privacy en bescherming van persoonsgegevens**: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.**Dit statement is de verbindende schakel tussen informatiebeveiliging en privacy. IB is een wettelijke eis om zorgvuldig met persoonsgegevens om te gaan.** |
| **Privacy toets:** privacy kan onderdeel zijn van het informatiebeveiligingsbeleid zoals opgenomen in statement 1.1. |

### Cluster 2: Personeel, studenten en gasten

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **2.1** | **7.1.2** | **Arbeidsvoorwaarden**: De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden. |
| **Privacy toets:** geen aanvullende opmerkingen |
| **2.2** | **7.2.2** | **Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging:** Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. |
| **Privacy toets:** geen aanvullende opmerkingen |
| **2.3** | **9.2.6** | **Toegangsrechten intrekken of aanpassen:** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast. |
| **Privacy toets:** de autorisatie matrix is voor dit statement cruciaal. Met name de medewerkers dit uitdienst zijn getreden moeten worden ge-audit. |
| **2.4** | **11.2.9** | **‘Clear desk’- en ‘clear screen’-beleid**: Er behoort een ‘clear desk’-beleid voor papieren documenten en verwijderbare opslagmedia en een ‘clear screen’-beleid voor informatie verwerkende faciliteiten te worden ingesteld. |
| **Privacy toets:** geen aanvullende opmerkingen |
| **2.5** | **13.2.4** | **Vertrouwelijkheids- of geheimhoudingsovereenkomst:** Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd. |
| **Privacy toets:** geheimhoudingsovereenkomst beoordelen. Onderzoek met name de deelnemersadministratie. T.a.v. de geheimhouding kan ook verwezen worden naar de cao.  |

### Cluster 3: Ruimtes en apparatuur

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **3.1** | **6.2.1.2** | **Beleid voor mobiele apparatuur:** Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico’s die het gebruik van mobiele apparatuur met zich meebrengt te beperken. |
| **Privacy toets:** een reglement notebooks (die eigendom zijn van de mbo instelling) is niet voldoende. Een AUP (Acceptable Use Policy), in het Nederlands “Verantwoord Netwerk Gebruik”, is noodzakelijk, immers alle medewerkers thuis op hun eigen device inloggen op applicaties die eigendom zijn van de mbo instelling moeten alle medewerkers zich aan de afspraken zoals verwoord in AUP houden. Juridisch is de AUP een aanvulling op de arbeidsovereenkomst als deze goedgekeurd is door de Ondernemingsraad (WOR, artikel 27, lid K). |
| **3.14** | **11.2.7** | **Veilig verwijderen of hergebruiken van apparatuur:** Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven. |
| **Privacy toets:** het betreft hier afvoer van apparatuur. |

### Cluster 4: Continuïteit

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **4.5** | **12.3.1.1** | **Back-up van informatie:** Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt.  |
| **Privacy toets:** controle van de volume van de back up is gewenst (Is van alle informatie een back up gemaakt?). Controleer logboek back up. |
| **4.6** | **12.3.1.2** | **Back-up van informatie:** Gemaakte back ups worden regelmatig getest conform het back-up beleid. |
| **Privacy toets:** terugzetten van bestanden (restore) middels een logboek controleren. |
| **4.14** | **17.1.2** | **Informatiebeveiligingscontinuïteit implementeren:** De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen. |
| **Privacy toets:** een continuïteitsplan (BCM) moet voorhanden zijn. |

### Cluster 5: Vertrouwelijkheid en integriteit

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **5.1** | **9.1.1** | **Beleid voor toegangsbeveiliging:** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. |
| **Privacy toets:** toegangsbeveiliging zowel voor het netwerk als voor applicaties**.** |
| **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. |
| **Privacy toets:** het betreft hier technische netwerkdiensten, denk aan VPN en draadloos netwerk. |
| **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. |
| **Privacy toets:** het betreft nieuwe gebruikers en het verwijderen van gebruikers. |
| **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. |
| **Privacy toets:** het verlenen van toegangsrechten tot applicaties op basis van functie en rollen (RBAC) van medewerkers. |
| **5.5** | **9.2.3** | **Beheren van speciale toegangsrechten:** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst. |
| **Privacy toets:** het betreft hier de super users / administrators rechten. |
| **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. |
| **Privacy toets:** het betreft het wachtwoorden beleid dat op basis van delegatie is goedgekeurd. |
| **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. |
| **Privacy toets:** geen aanvullende opmerkingen. |
| **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. |
| **Privacy toets:** de gebruiker ziet alleen die opties in het keuzemenu waartoe hij rechten heeft. |
| **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. |
| **Privacy toets:** een aantal aanbevelingen:* 2-way authenticatie;
* Wachtwoord kan niet worden “afgeluisterd”;
* Wachtwoord wordt niet weergegeven;

Wachtwoord en username komen niet overeen is de juiste foutmelding bij onjuist ingetypt wachtwoord. |
| **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. |
| **Privacy toets:** beleid t.a.v. digitale sleutels (voorbeeld Bitlocker). |
| **5.11** | **10.1.2.2** | **Sleutelbeheer:** Er wordt gebruik gemaakt van tools om cryptografische sleutels tijdens hun gehele levenscyclus adequaat te beheren. |
| **Privacy toets:** beheer van digitale sleutels (bijvoorbeeld Bitlocker). |
| **5.12** | **12.4.2** | **Beschermen van informatie in logbestanden:** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. |
| **Privacy toets:** geen aanvullende opmerkingen |
| **5.16** | **13.2.3** | **Elektronische berichten**: Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd |
| **Privacy toets:** toetsen op certificering. |

### Cluster 6: Controle en logging

|  |  |  |
| --- | --- | --- |
| **Nr.** | **ISO27002** | **Statement** |
| **6.1** | **9.2.5** | **Beoordeling van toegangsrechten van gebruikers:** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. |
| **Privacy toets:** een van de belangrijkste statements. De proceseigenaar moet samen met hoofd systeembeheer controleren of de toegangsrechten juist zijn. |
| **6.2** | **12.4.1** | **Gebeurtenissen registreren:** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. |
| **Privacy toets:** geen aanvullende opmerkingen. |
| **6.9** | **18.2.2** | **Naleving van beveiligingsbeleid en –normen:** Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging. |
| **Privacy toets:** proceseigenaren controleren of afspraken gerealiseerd zijn. Er mogen geen vragen zijn in de trant van: “Waar liggen de verantwoordelijkheden?”. |
| **6.10** | **18.2.3** | **Beoordeling van technische naleving:** Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging. |
| **Privacy toets:** beoordeling op technisch inhoudelijk gebied.. |

# Normenkader examinering

In wet- en regelgeving vanuit de overheid op het gebied van examinering binnen het mbo zijn informatiebeveiligingsaspecten opgenomen. Vanuit die wet- en regelgeving zijn de normen geformuleerd:

|  |
| --- |
| WEB = wet educatie en beroepsonderwijs  |
| TK12 = toetsingskader '12 TKA15 = addendum '15 |
| RECE'15 = regeling examenprotocol centrale examinering |
| RMD = regeling modeldiploma |
| HRSE = handreiking onregelmatigheden servicepunt |

Naast de betreffende informatiebeveiligingsaspecten zijn er in de wet- en regelgeving over examinering ook kwaliteitsaspecten die geregeld moeten zijn. Maar deze vallen geheel buiten het kader van informatiebeveiliging. Meer informatie over de kwaliteitsaspecten kan verkregen worden via het servicepunt examinering van de MBO Raad. In samenwerking met de MBO Raad is van de informatiebeveiligingsaspecten een set van informatiebeveiligingsnormen gemaakt.

Veel van de vereiste informatiebeveiligingsaspecten komen terug in de statements van het normenkader informatiebeveiliging mbo, dat gebaseerd is op ISO 27002. Het kan dan ook gezegd worden dat allereerst de generieke informatiebeveiliging op orde moet zijn.

Voor examinering is er een aantal statements dat meer aandacht nodig heeft of een hoger niveau van het vervullen van de betreffende norm nodig heeft. Hieruit volgen 17 gemeenschappelijke statements voor informatiebeveiliging en examinering. Waar bij het algemene toetsingskader informatiebeveiliging wellicht een niveau 2 voldoende is, is het in het kader van examinering van belang om hier naar een hoger ambitieniveau te streven, bijvoorbeeld een niveau 3 of zelfs 4.

Naast deze gemeenschappelijke statements is er op basis van eerder genoemde wet- en regelgeving ook een aanvullende set van statements opgesteld. Een deel hiervan is van toepassing op al bestaande processen uit het pre-digitale tijdperk. Die zijn wel opgenomen in de bijlage maar spelen in het voorliggende toetsingskader geen rol. In het kader van het programma informatiebeveiliging en privacy gaat het vooral om examinering waarbij de inzet van ict een rol speelt: digitale versies van examens en digitaal examens afnemen. De daarbij behorende informatiebeveiligingsaspecten zijn uitgewerkt in **17** statements, die nader zijn uitgewerkt in het toetsingskader examinering conform de MBOaudit werkwijze.

## Basisprincipes examinering

Om het toetsingskader examinering goed te plaatsen, is het belangrijk de basisprincipes van examinering te kennen. Hieronder volgt een korte samenvatting.



De Procesarchitectuur Examinering (PE) is een schematische weergave van het hele examenproces in het mbo. Alle stappen die een mbo-instelling moet nemen om te zorgen voor goede examinering, komen aan de orde. Denk bijvoorbeeld aan het opstellen van het examenplan, inkopen en/of zelf samenstellen van examens, diplomeren en borgen van de examenkwaliteit. De PE helpt instellingen om kritisch naar hun eigen examen-proces te kijken.

De PE bestaat uit zes procesgebieden met ieder een eigen, herkenbare kleur. Ieder procesgebied bevat onderliggende processtappen. Op de site van het servicepunt examinering van de MBO Raad staat de meest recente en digitale variant van de PE. Bij het realiseren van een goede examenkwaliteit is het uitvoeren (do) wellicht de kern, maar er is pas sprake van borging als er ook een goede planfase (plan), een degelijke evaluatie (check) en adequate bijstelling (act) zijn. Dit is de zogeheten pdca-cyclus.

In het schema van de PE zijn de plan-, check- en actfase dan ook aan de gekleurde procesgebieden toegevoegd en uitgewerkt..

## Statements normenkader examinering

### Dit beleid is afgeleid van het document Kwaliteitsborging Examineren.

|  |  |  |
| --- | --- | --- |
| **E.1** | WEB Art. 7.4.4 Art. 7.4.8.1-2. TK12; 2.1.5., 2.2.1., 2.3.2. RECE '15; (1, 2, 6-17, 18, 19) RMD HRSE; p. 5-7, p. 11-12 | **Beleidsregels examinering**Voor de informatiebeveiliging van examinering moeten beleidsregels worden gedefinieerd, goedgekeurd door het CvB, gepubliceerd en gecommuniceerd aan medewerkers en andere betrokkenen. |
| **E.2** | WEB Art. 7.4.4.2., Art. 7.4.8.1-2. TK12; 2.1.5., 2.3.2. RECE '15; (6-17) RMD HRSE; p.5-7 | **Richtlijnen bij constatering fraude bij digitale examens**Het handelen bij de constatering van onregelmatigheden en fraude moet volgens een vastgestelde standaardrichtlijn te geschieden.  |
| **E.3** | WEB Art. 7.4.4.2., Art. 7.4.8.1., Art. 7.4.8.5. TK12; 2.1.5., 2.3.2. RECE '15; (1) (6-17) RMD Art. 5 HRSE; p. 5-6 | **Procesaanpassing bij digitale examens m.b.t. examenfraude**Om examenfraude in de toekomst te voorkomen moeten passende procedures worden ontwikkeld en geïmplementeerd die in overeenstemming zijn met het vastgestelde examenreglement van de organisatie.  |
| **E.4** | WEB Art. 7.2.6.2 Art. 7.4.4. Art. 7.4.5 Art. 7.4.8.5 TK12; 2.1.5.,2.2.2, 2.3.2. RECE '15; (1-5, 11-12) RMD HRSE; p. 4-6, p. 8, p. 11, p 14 | **Procedure ontwikkelen examinering in beveiligde omgeving**Inkoop, ontwikkeling of hergebruik van examens dienen volgens vastgestelde standaardprocedures uitgevoerd te worden, uitsluitend door daartoe bevoegde en bekwame personen met een hiertoe vastgestelde taak.  |
| **E.5** | WEB Art. 7.4.3 - 3a Art. 7.4.4 Art. 7.4.4.2., Art. 7.4.8. Art. 7.4.8.5 TK12; 2.1.5, 2.2.1, 2.2.2, 2.3.2. RECE '15; (1, 2, 5, 6-17, 19) RMD HRSE; p. 4-5, p. 11, p. 12 | **Procedure voorbereiden en afnemen examens**Bij de voorbereiding en bij het afnemen van examens worden ict faciliteiten op gestructureerde wijze gereserveerd en ingezet |
| **E.6** | WEB Art. 7.4.4.2. TK12; 2.1.5, 2.2.2., 2.3.2. RECE '15; (1, 11, 18) RMD HRSE; p. 14 | **Eindevaluatie examenproces en de integriteit van resultaten**Er moet een eindevaluatie ingeregeld zijn om te beoordelen of eindresultaten conform verwachtingen zijn of dat er wellicht fraude of onregelmatigheden zijn geconstateerd.  |

###  Aanvullende statements gerelateerd aan personeel

|  |  |  |
| --- | --- | --- |
| **E.7** | WEB Art. 7.4.4., Art. 7.4.4a.1-2. TK12; 2.1.5, 2.3.2. RECE '15; nvt RMD HRSE; p. 4-5, 11, 14 | **Gedragscodes, inclusief richtlijnen**Er dienen gedragscodes of -richtlijnen te zijn omtrent examenafname en de omgang met examengegevens. Deze richtlijnen dienen ingevoerd te zijn voor interne en externe betrokkenen.  |
| **E.8** | WEB Art. 7.1.2.2. Art. 7.4.4 Art 7.4.8TK12; 2.1.5, 2.2.2., 2.3.2. RECE '15; (12) RMD HRSE; p. 4-5, 8-10, 14 | **Extra ondersteuning bij examens.**Extra ondersteuning bij examens voortvloeiend uit een zorgdossier vindt alleen plaats aan de hand van vastgelegde afspraken op individueel niveau.  |
| **E.9** | WEB Art. 7.4.4. TK12; 2.1.5, 2.2.2., 2.3.2. RECE '15; (2-17) RMD HRSE; p. 9 | **Trainingen en vaardigheden m.b.t fraude bij digitale examens**Bij het afnemen van examens dient personeel ingezet te worden met voldoende vaardigheden met betrekking het correct laten verlopen van de examens en tot het herkennen van mogelijke fraude en het adequaat afhandelen daarvan. |

### Aanvullende statements gerelateerd aan uitvoering

|  |  |  |
| --- | --- | --- |
| **E.10** | WEB Art. 7.4.4., Art. 7.4.8. TK12; 2.1.5, 2.2.2., 2.3.2. RECE '15; (1) (4) RMD HRSE; p. 8-10 | **Beveiligde examenruimte**De examenomgeving (fysiek en digitaal) dient beveiligd te zijn tegen fraude en/of onregelmatigheden.  |
| **E.11** | WEB Art. 7.4.4., Art. 7.4.8. TK12; 2.1.5, 2.2.2., 2.3.2. RECE '15; (1) (2-5) RMD HRSE; p. 8-10 | **Faciliteiten voor examen**Het beschikbaar stellen van de faciliteiten voor examens en het hanteren van deze faciliteiten dient volgens een vastgestelde standaardprocedure te verlopen. |
| **E.12** | WEB Art. 7.4.4., Art. 7.4.8. TK12; 2.1.5, 2.2.2., 2.3.2. RECE '15; (1) (2) RMD HRSE; p. 8-10 | **Hanteren van digitaal examenmateriaal** Het veilig omgaan met en het beschikbaar stellen van examenmateriaal dient volgens een vastgestelde standaardprocedure te verlopen.  |
| **E.13** | WEB Art. 7.4.4., Art. 7.4.8. TK12; 2.1.5, 2.2.2., 2.3.2. RECE '15; (1) (5, 7) RMD HRSE; p. 12, 14 | **Continuïteitsplan**Voor resources die op het moment van examinering beschikbaar moeten zijn, of waarnaar in aanloop naar de examinering een kritieke tijdsafhankelijke relatie bestaat, is een continuïteitsplan beschikbaar. |
| **E.14** | WEB Art. 7.4.4., Art. 7.4.8. TK12; 2.1.5, 2.2.2., 2.3.2. RECE '15; (1) (5, 18, 19) RMD HRSE; p. 12-13 | **Toekennen examens aan deelnemers**De toekenning van examens aan deelnemers en de controle op naleving daarvan moet via een veilige procedure verlopen. |
| **E.15** | WEB Art. 7.4.8. TK12; 2.1.5, 2.2.2., 2.3.2. RECE '15; (1) nvt RMD HRSE; p. 4-5, 7 | **Hergebruik examenvragen**Bij hergebruik van examens dient er een verscherpte beveiliging te zijn om kopiëren tegen te gaan.  |
| **E.16** | WEB Art. 7.4.4. TK12; 2.1.5, 2.3.2. RECE '15; (1) (2) (12) RMD HRSE; p. 4-5, 8-9 | **Vernietigen examenmateriaal**Het vernietigen van examenmateriaal (vragen, gemaakte examens, concepten en hulpmateriaal) dient op een effectieve en veilige manier te gebeuren met inachtneming van de eisen voor bewaartermijnen.  |

## Statements examinering afgeleid van het ib normenkader

### Generieke statements voorafgaande aan examinering

|  |  |  |
| --- | --- | --- |
| **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. |
| **Toelichting examineren:**Beveiligingsaspecten opnemen in de leveranciersovereenkomsten voor digitale examens, bijvoorbeeld in SLA vorm met zaken als beschikbaarheid, performance, logging van handelingen van gebruikers en veilige koppeling van gegevens. Voor privacy aspecten geldt de noodzaak van een bewerkersovereenkomst |
| **1.17** | **16.1.1** | **Verantwoordelijkheden en procedures**: Er zijn leidinggevende en -procedures vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.  |
| **Toelichting examineren:**Informatiebeveiligingsincidenten in het kader van digitaal examineren worden geregistreerd en er is een afhandelingsproces gedefinieerd waarin taken, verantwoordelijkheden en bevoegdheden zijn belegd. |
| **1.18** | **16.1.2** | **Rapportage van informatiebeveiligingsgebeurtenissen**: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. |
| **Toelichting examineren:**Informatiebeveiligingsincidenten in het kader van digitaal examineren worden gerapporteerd. |
| **1.19** | **18.1.3** | **Beschermen van registraties**: Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave. |
| **Toelichting examineren:**Registraties van digitale examens en de bewaartermijnen voldoen aan wet- en regelgeving. |
| **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. |
| **Toelichting examineren:**Er moet een passende toegangsbeveiliging zijn voor systemen waarin examenmateriaal is opgeslagen. Dit omvat gebruikersbeheer, passende autorisaties, inlogprocedures, het loggen van inlog(pogingen). Inlogprocedures voor digitale examens voldoen aan de wet- en regelgeving van een mbo instelling |

### Generieke statements tijdens het proces van examinering

|  |  |  |
| --- | --- | --- |
| **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. |
| **Toelichting examineren:**Er is beleid nodig voor het adequaat afschermen van examineringsgegevens d.m.v. het toepassen van cryptografische beheersmaatregelen (versleutelen bij transport en opslag van data). |
| **1.10** | **10.1.1.2** | **Beleid inzake het gebruik van crypto grafische beheersmaatregelen:** Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van crypto grafische beheersmaatregelen wordt geïmplementeerd. |
| **Toelichting examineren:**Alle medewerkers betrokken bij examineren maken gebruik van versleutelingstechnieken conform het beleid. |

|  |  |  |
| --- | --- | --- |
| **2.3** | **9.2.6** | **Toegangsrechten intrekken of aanpassen:** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, bij wijzigingen behoren ze te worden aangepast. |
| **Toelichting examineren:**Toegangsrechten tot systemen met examineringsgegevens worden uitgegeven/ingetrokken volgens vastgestelde procedures/beleid. |
| **2.4** | **11.2.9** | **‘Clear desk’- en ‘clear screen’-beleid**: Er behoort een ‘clear desk’-beleid voor papieren documenten en verwijderbare opslagmedia en een ‘clear screen’-beleid voor informatie verwerkende faciliteiten te worden ingesteld. |
| **Toelichting examineren:**Alle medewerkers met toegang tot examineringsgegevens hanteren een “clear desk” en “clear screen”-beleid. |
| **3.5** | **11.1.3** | **Kantoren, ruimten en faciliteiten beveiligen:** Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast. |
| **Toelichting examineren:**Er is een fysieke beveiliging van ruimten waar examens worden geconstrueerd en afgenomen. |
| **4.13** | **16.1.5** | **Respons op informatiebeveiligingsincidenten:** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures. |
| **Toelichting examineren:**Beveiligingsincidenten die geregistreerd zijn bij de afname van digitale examens worden adequaat opgelost. |
| **4.15** | **17.2.1** | **Beschikbaarheid van informatie verwerkende faciliteiten:** Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen. |
| **Toelichting examineren:**Er zijn voorzieningen getroffen (zoals reserve apparatuur) zodat examens bij bijv. korte netwerkstoringen of een defecte PC kunnen doorgaan. |
| **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. |
| **Toelichting examineren:**Er is een beleid geformuleerd voor de toegang van digitale examens. |
| **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. |
| **Toelichting examineren:**Deelnemers die hun examen hebben afgerond worden geregistreerd en afgemeld. |
| **5.12** | **12.4.2** | **Beschermen van informatie in logbestanden:** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. |
| **Toelichting examineren:**Logbestanden van de afname digitale examens, van toegang tot examenmateriaal en tot examenresultaten zijn beschermd tegen inbreuk en onbevoegde toegang. |
| **6.1** | **9.2.5** | **Beoordeling van toegangsrechten van gebruikers:** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. |
| **Toelichting examineren:**De toegangsrechten tot examens en examenconstructie worden regelmatig beoordeeld. |
| **6.2** | **12.4.1** | **Gebeurtenissen registreren:** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. |
| **Toelichting examineren:**Activiteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen van medewerkers die examineringsgegevens inzien of bewerken moeten worden geregistreerd (gelogd) en beoordeeld. |
| **6.3** | **12.4.3** | **Logbestanden van beheerders en operators:** Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld. |
| **Toelichting examineren:**Activiteiten van gebruikers die bij examengegevens kunnen, moeten worden gelogd. |

# http://www.blikopnieuws.nl/sites/default/files/artikel/digid-code-logo.jpgNormenkader digitaal ondertekenen

Het bedrijf Evidos biedt de ondertekendienst ‘Ondertekenen.nl’ aan. SURFmarket heeft met Evidos voor de instellingen een bemiddelingsovereenkomst gesloten aan de hand van het Juridische Normenkader Cloudservices Hoger Onderwijs. In de bemiddelingsovereenkomst is opgenomen dat Evidos voldoet aan beveiligingseisen en een ‘Third Party Memorandum’ (TPM) over haar dienstverlening oplevert. SURFmarket en Evidos hebben aangegeven in nadere afspraken vast te leggen dat Evidos jaarlijks een DigiD assessment rapport oplevert over haar DigiD dienstverlening (een zogenaamd ‘DigiD TPM’).

De normen voor het DigiD assessment zijn 28 beveiligingsrichtlijnen gebaseerd op de (NCSC) ict-beveiligingsrichtlijnen voor web applicaties van het Nationaal Cyber Security Centrum. De richtlijnen betreffen de governance, het applicatie- en infrastructuurbeheer van de ondertekendienst bij de instelling en de ict-serviceprovider.

Voor mbo instellingen is het belangrijk om te weten welke richtlijnen voor hen van belang zijn. Daarom zijn de richtlijnen opgenomen als statements. De instelling is zelf verantwoordelijk voor zeven DigiD statements. Zes van de zeven statements worden door 22 statements uit het normenkader informatiebeveiliging mbo afgedekt. Omdat één statement (wachtwoordbeleid) niet in het toetsingskader ib is opgenomen, is dit alsnog toegevoegd.

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 en verslaggeving van de instelling. Aangezien deze financiële informatie in de meeste gevallen rechtstreeks uit geautomatiseerde informatiesystemen komt, 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 vaststellen of de instelling voldoende algemene maatregelen binnen de (automatiserings-)organisatie heeft genomen om de betrouwbare en continue werking van de geautomatiseerde informatiesystemen te waarborgen (de zogenaamde ‘General Computer Controls’ (GCC)).

## Basisprincipes digitaal ondertekenen

Instellingen zijn en blijven eigenaar van de gegevens in de ondertekendienst. Een instelling moet over deze gegevens kunnen beschikken als 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 moet jaarlijks een DigiD assessment uit laten voeren.

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 Evidos waarmee de algemene voorwaarden van toepassing worden verklaard op de dienstverlening van Evidos aan de instelling. Deze overeenkomsten vormen een goede basis voor het DigiD assessment.

## Statements DigiD

### 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. | 5.15.25.35.45.55.65.75.85.9Niet in gebruik | 9.1.19.1.29.2.19.2.29.2.39.2.49.3.19.4.19.4.2**9.4.3** |
| Op basis van inspectie wordt vastgesteld op 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. | 1.154.11 | 15.1.215.2.2 |
| Met Evidos 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 normenkader is op voldoende niveau. |
| **B 5-1** | Voer sleutelbeheer in waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers te vinden zijn. | 1.9 en 1.105.10 en 5.11 | 10.1.110.1.2 |
| 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 1.105.10 en 5.11 | 10.1.110.1.2 |
| 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 1.21.31.4 | 5.1.15.1.26.1.1 |
| Een goedgekeurd en gecommuniceerd ibp beleidsplan moet aanwezig zijn. Dit beleidsplan moet in een PDCA cyclus zijn opgenomen. |

### NOREA-beveiligingsrichtlijnen voor Evidos

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

* 1. **Informatiebeveiliging-statements ter onderbouwing NOREA-beveiligingsrichtlijnen voor de instelling**

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

|  |  |  |
| --- | --- | --- |
| **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 één 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 wordt daarom aangeraden 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 w 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 kritische 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 |

Verantwoording

**Auteurs**

Leo Bakker (Kennisnet)

Ludo Cuijpers (Kennisnet)

Versie 3.0 september 2017

**Sommige rechten voorbehouden**

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgever van Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.

Op teksten in deze publicatie rust mogelijk auteursrecht van derden. Dat betekent dat het niet is toegestaan om zonder voorafgaande toestemming van Kennisnet of saMBO-ICT teksten uit deze publicatie over te nemen, te bewerken, of verder (digitaal) te verspreiden. De elders in het framework ibp gebruikte CC-BY licentie is op dit document niet van toepassing.

**Framework informatiebeveiliging en privacy in het mbo**



1. **I**nformatie**b**eveiliging en **p**rivacy [↑](#footnote-ref-1)
2. https://www.surf.nl/kennisbank/2015/beleidsnotitie-modelbeleid-en-procedure-responisible-disclosure.html [↑](#footnote-ref-2)
3. NTP: network time protocol [↑](#footnote-ref-3)
4. Privacy by design houdt in dat de organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht besteedt aan privacyverhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. (bron; CBP) [↑](#footnote-ref-4)