Deze analyse is opgesteld om het bestaande uitgifteproces van accounts binnen het onderwijs te toetsen tegen het (eIDAS) betrouwbaarheidsniveau Laag. Dit op basis van een Toetsmatrijs eIDAS Substantieel (zie [NEN NCS7516](https://www.nen.nl/ncs-7516-1-2020-nl-268924)[[1]](#footnote-2)). Aangezien het tegenover het niveau Laag getoetst moet worden, is gekeken naar de verschillen tussen Laag en Substantieel (die op te maken zijn uit de [eIDAS verordening](https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32015R1502&from=NL)). Op basis daarvan zijn de wijzigingen doorgevoerd (zie voorgestelde wijziging in de eerste kolom ‘Elementen’). Vervolgens is de ‘Toepassing op het onderwijs’ uitgewerkt. In sommige gevallen een controle vraag (die door de onderwijsinstelling gecontroleerd moet worden) of in een aanname waarbij dit reeds van toepassing is binnen bestaande processen, zoals het inschrijf- of indienstproces. Als voorbeeld van invulling van de voorschriften, is het [Afsprakenstelsel eToegang](https://afsprakenstelsel.etoegang.nl/display/as/Technische+specificaties+en+procedures+voor+uitgifte+van+authenticatiemiddelen) geraadpleegd. Op alle vragen dient Ja beantwoord te worden om compliant te zijn.

|  |  |  |
| --- | --- | --- |
| ***Elementen*** | **eIDAS**  **Laag** | ***Toepassing op het onderwijs*** |
| **Inschrijving** |  | **Op welke wijze de inschrijving is verzorgt, waarbij de gebruiker wordt geïnformeerd en de identiteit van de gebruiker op de juiste wijze - met bewijs - gecontroleerd wordt. Hierbij kan grotendeels geleund worden op wettelijke eisen omtrent inschrijving van enerzijds medewerkers en anderzijds leerling/student.** |
| *Aanvraag en registratie* |  |  |
| Is elke aanvrager bekend met de voorwaarden die aan het gebruik van het elektronische identificatiemiddel zijn verbonden? | 2.1.1  Punt 1 | *Controle vraag:* Zijn de leerlingen/studenten en medewerkers bekend met de voorwaarden en veiligheidsvoorzorgen die aan het gebruik van het inlogmiddel zijn verbonden?  *Mogelijk antwoord:* Ja, als dit onderdeel van het gedragscode wat voor zowel de leerling/student als medewerker geldt.  *Zie ook Toetsingskader/ISO27002 7.1.2 Arbeidsvoorwaarden* |
| Is hij bekend met de aanbevolen veiligheidsvoorzorgen die aan het gebruik van het elektronische identificatiemiddel zijn verbonden? | 2.1.1  Punt 2 | Zie hierboven. |
| Worden de relevante identiteitsgegevens die voor het bewijs en de verificatie van de identiteit vereist zijn, verzameld? | 2.1.1  Punt 3 | *Aanname:* Ja, tijdens het inschrijfproces van de leerling worden de gegevens (BSN, geboortedatum, geslacht en postcode of landcode) overgenomen van het identiteitsbewijs, geboorteactie, o.i.d. De naam en BSN wordt vervolgens door BRON aangeleverd en in het LAS opgeslagen.  Voor een medewerker worden de gegevens overgenomen van een paspoort bij indiensttreding. Daarbij is de werkgever tevens verplicht een kopie van het paspoort te maken. |
| *Bewijs en verificatie van de identiteit van een natuurlijk persoon* |  |  |
| Kan er verondersteld worden dat de persoon in het bezit is van een geldig EU-paspoort of een in Nederland uitgegeven rijbewijs of identiteitsbewijs? | 2.1.2 | *Leerlingen en Studenten*  *N.v.t. voor alle leerlingen:* het is niet verplicht om een ID of paspoort te hebben als kind (onder de 14 jaar)[[2]](#footnote-3). Daarnaast kunnen ook niet EU-burgers zich inschrijven op een schoolinstelling. Bijvoorbeeld door asielzoekers of internationale studenten.  ***Keuze maken:***  *Om voor leerling/student ook alternatieve bewijzen toe te staan: bv. die ook gebruikt worden bij het inschrijven, zoals geboortebewijs of uitschrijfbewijs (PO/VO). Inschrijving van HO vindt plaats via Studielink en biedt daarmee voldoende zekerheid?*  *Medewerkers*  *Aanname: er kan verondersteld worden dat medewerkers een EU-paspoort kunnen hebben want alleen Europese burgers mogen werkzaam zijn. Er geldt echter een uitzondering voor bijvoorbeeld asielzoekers.* |
| Kan verondersteld worden dat het bewijs echt kan zijn, dan wel volgens een gezaghebbende bron te bestaan, en het bewijs lijkt geldig te zijn? | 2.1.2 | *Niet van toepassing voor alle leerlingen:* kinderen onder de 14 jaar zijn niet verplicht een identiteitsbewijs te hebben. Wel kunnen zij een ander bewijs hebben, zoals een geboortebewijs. Het bewijs controleren bij inschrijving is geen verplichting vanuit de wet.  *Leerling/Student* *Controle vraag: wordt het alternatieve bewijs gecontroleerd op echtheid en geldigheid OF wordt dit gecontroleerd volgens een gezaghebbende bron?*  Medewerker  *Aanname:* voor (nieuwe) medewerkers geldt zelf een identificatieplicht[[3]](#footnote-4), waarbij het identificatiebewijs op echtheid en geldigheid wordt gecontroleerd. |
| Wordt de opgegeven identiteit gecontroleerd op bestaan in een gezaghebbende bron en kan er verondersteld worden dat de persoon die de identiteit opgeeft, dezelfde persoon is? | 2.1.2 | *Leerling/Student Aanname:* Ja, bij het inschrijven van de leerling in BRON worden de identiteitsgegevens gecontroleerd die zijn aangereikt door de (ouders van de) leerling. Hiervoor hanteert BRON het Basis administratie Personen (BAP). Die controleert o.a. met Basis Registratie Personen (BRP).  Medewerker  *Aanname (voldoet niet)*: Dat geldt niet voor een medewerker, aangezien daarvan alleen de identiteit gecontroleerd wordt maar niet het bestaan in een gezaghebbende bron zoals BRP of RNI. Wel wordt een medewerker aangemeld bij de belastingdienst, echter is dit niet bedoeld voor controle.  ***Keuze maken:*** *Om voor medewerker te vertrouwen op de controle van het bewijs. Dit gebeurt reeds op een hoger niveau dan nodig voor Laag. Het bewijs wordt immers gecontroleerd op echtheid en geldigheid en er wordt een kopie van gemaakt. Het risico dat een medewerker in dienst komt met een nagemaakt paspoort is immers erg klein.* |
| (Mogelijk zijn uitzonderingen van toepassing, zie UeIDAS A.1.2.) |  |  |
| *Bewijs en verificatie van de identiteit van een rechtspersoon* |  |  |
| Wordt de opgegeven identiteit van de rechtspersoon aangetoond aan de hand van een recent uittreksel van het Handelsregister? | 2.1.3 | *Niet van toepassing* |
| Wordt gecontroleerd of het uittreksel geldig is en echt lijkt te zijn, of wordt het bestaan door het Handelsregister bevestigd? | 2.1.3 | *Niet van toepassing* |
| Wordt gecontroleerd of de rechtspersoon zich volgens het Centraal Insolventieregister niet in faillissementen of surseances van betaling bevindt? | 2.1.3 | *Niet van toepassing* |
| (Mogelijk zijn uitzonderingen van toepassing, zie UeIDAS A.1.3.) |  |  |
| Koppeling tussen de elektronische identificatiemiddelen van natuurlijke en rechtspersonen |  | *Niet van toepassing* |
| Wordt in het Curatele- en bewindregister gecontroleerd of de natuurlijke persoon niet onder curatele of bewind geplaatst is? | 2.1.4  punt 3 | *Niet van toepassing* |
| Wordt het identiteitsbewijs van de natuurlijke persoon geverifieerd conform het hierboven genoemde ‘Bewijs en verificatie van de identiteit van een natuurlijk persoon'? | 2.1.4  punt 1 | *Niet van toepassing* |
| Is de handelingsbevoegdheid van de natuurlijke persoon geverifieerd op basis van informatie uit het Handelsregister? | 2.1.4  Punt 2? | *Niet van toepassing* |
| **Beheer van elektronische identificatiemiddelen** |  | **De keuze voor het juiste inlogmiddel en de wijze waarop deze beheerd wordt, zoals uitgifte, schorsing, reactivering, verlening en vervanging.** |
| Kenmerken en ontwerp van elektronische identificatiemiddelen |  |  |
| Maakt het elektronische identificatiemiddel gebruik van minstens één authenticatiefactoren uit verschillende categorieën? | 2.2.1 | *Aanname: s*tandaard worden inlogmiddelen uitgegeven met één factorauthenticatie: gebruikersnaam en wachtwoord. |
| Is het elektronische identificatiemiddel ontworpen dat de uitgever ervan redelijke stappen onderneemt om te verifiëren dat het slechts wordt gebruikt door of onder controle staat van de bevoegde persoon (of kan dit worden verondersteld)? | 2.2.1 | *Controle vraag:* Wordt het wachtwoord op een veilige manier uitgegeven aan de gebruiker en wordt afgedwongen dat deze aangepast wordt naar een sterk wachtwoord (als de gebruiker deze voor de eerste keer gebruikt wordt)?  *Zie ook ISO27001 - A9.2.4 Beheer van geheime authenticatie-informatie van gebruikers* |
| Uitgifte, uitreiking en activering |  |  |
| Wordt het elektronische identificatiemiddel uitgereikt op een wijze waarmee alleen de bevoegde persoon het bereikt (of kan dit worden verondersteld)? | 2.2.2 | Zie hierboven. |
| Schorsing, herroeping en reactivering |  |  |
| Kan het elektronische identificatiemiddel snel en doeltreffend worden geschorst en/of herroepen? | 2.2.3 | *Controle vraag:* Kan het inlogmiddel snel (en opnieuw) ge(de)activeerd worden?  *Mogelijk antwoord:* Ja, (de)activeren is een standaard functionaliteit. |
| Zijn er maatregelen om ongeoorloofde schorsing, herroeping en reactivering te voorkomen? | 2.2.3 | *Controle vraag:  Is het proces voor uitgifte, uitreiking en activering is gedegen (met voldoende maatregelen) geïmplementeerd om ongeoorloofde schoring, herroeping of reactivering te voorkomen? Een risicoanalyse/audit op dit proces kan helpen om deze controle vraag te beantwoorden.* |
| Kan een reactivatie uitsluitend plaatsvinden als (nog steeds) wordt voldaan aan de betrouwbaarheidsvereisten die voorafgaand aan de schorsing of herroeping van kracht waren? | 2.2.3 | *Controle vraag:* Vind er een validatie plaats of het verzoek tot reactiveren (lees ook: wachtwoord reset) afkomstig is van een bevoegd persoon en of wordt daarbij de identiteit gecontroleerd? Een bevoegd persoon kan naast de gebruiker ook een bevoegde medewerker van de schoolinstellingen zijn. |
| Verlenging en vervanging |  |  |
| Wordt bij verlenging of vervanging aan dezelfde betrouwbaarheidsvereisten voldaan als voor het initiële proces van bewijs en verificatie van de identiteit, dan wel wordt uitgegaan van een geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau ‘laag’, ‘substantieel’ of ‘hoog’? | 2.2.4 | *Aanname*: een gebruikersaccount wordt onder normale omstandigheden niet verlengd (verloopt niet). Wel kan het wachtwoord veranderen, waarbij het huidige wachtwoord nodig is om de identiteit vast te stellen. Als dit als een ander verzoek binnenkomt, geldt de controle vraag die ook geldt bij reactiveren (2.2.3). |
| Wordt daarbij rekening gehouden met het risico dat de persoonsidentificatiegegevens zijn gewijzigd? | 2.2.4 | *Aanname:* dit is niet van toepassing. Een gebruikersaccount wordt onder normale omstandigheden niet verlengd (verloopt niet) en opnieuw aangemaakt. Wanneer een leerling van school wijzigt, volgt opnieuw het inschrijfproces en dus uitgifteproces met daarbij het identificatieproces.  Wel staat het de leerling/student en medewerker vrij, om zijn of haar naam wijziging door te geven. Identiteitsgegevens moeten dan gecontroleerd worden.  *Controle vraag:* Wordt er bij een naamswijziging de identiteitsgegevens opnieuw gevalideerd, zoals bij inschrijving plaatsvindt? |
| **Authenticatie** |  | **De wijze waarop de authenticatiemechanisme functioneert. Dit wordt ingevuld door de techniek.** |
| Authenticatiemechanisme |  |  |
| Worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd voordat persoonsidentificatiegegevens worden vrijgegeven? | 2.3.1  Punt 1 | *Aanname:* Ja, dit is een standaard functionaliteit. Pas na een succesvol inloggen, worden eventueel persoonsgegevens getoond in een (selfservice) portaal of applicatie. |
| Als er in het authenticatiemechanisme persoonsidentificatiegegevens worden opgeslagen, worden die gegevens dan beveiligd tegen verlies en schending, inclusief offlineanalyse? | 2.3.1  Punt 2 | Dit is afhankelijk van de gebruikte software van het inlogmiddel.  *Controle vraag:* Is de gebruikte software en techniek beveiligd tegen bedreigingen en misbruik? Dit kan een voorwaarden of garantie zijn van de leverancier en of uitkomst van een risicoanalyse/pentest bij inzet van eigen software en/of techniek. |
| Voorziet het authenticatiemechanisme in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatie mechanismen kunnen worden omzeild door middel van gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een laag aanvalspotentieel? | 2.3.1  Punt 3 | Zie hier boven. |
| **Beheer en organisatie** |  | **De inrichting van beheer en organisatie voor informeren van gebruikers, bijhouden van administratie en inrichting van informatiebeveiliging omtrent faciliteiten, personeel en techniek incl. de controle en audit ervan. Verder algemene bepalingen waarmee ingestemd moet worden, wat ingevuld kan worden door de sector.** |
| Algemene bepalingen |  |  |
| Is de aanbieder die een operationele dienst aanbiedt onder eIDAS, een overheidsinstantie of een rechtspersoon volgens Nederlands recht? | 2.4.1 | *Aanname:* Ja, een schoolbestuur betreft een rechtspersoon. |
| Beschikt de aanbieder over een gevestigde organisatie? | 2.4.1 | *Aanname:* Ja, een schoolinstelling is altijd een gevestigde organisatie |
| Is de aanbieder volledig operationeel op alle gebieden die voor de dienstverlening relevant zijn? | 2.4.1 | *Besluiten om dit onderdeel te laten zijn van een toetredingsovereenkomst of afspraak binnen de sector.* |
| Voldoet de aanbieder aan al zijn wettelijke verplichtingen vanwege zijn dienstverlening (o.a. de soorten informatie die mogen worden gevraagd, de wijze waarop bewijs van identiteit wordt geleverd, welke informatie mag worden bewaard en hoe lang deze mag worden bewaard)? | 2.4.1 | *Aanname:* Ja, met het inschrijf- en in-dienstproces moeten (wettelijk) persoonsgegevens opgevraagd en gecontroleerd worden. |
| Heeft de aanbieder aangetoond in staat te zijn het risico van de aansprakelijkheid voor schade op zich te nemen en over voldoende financiële middelen te beschikken om zijn activiteiten en de dienstverlening voort te zetten? | 2.4.1 | *Besluiten of deze eis wel benodigd is voor de toepassing binnen het onderwijs. Een cyberverzekering kan dit eenvoudig afdekken, echter is de vraag of de aansprakelijkheid bij enige fouten wel bij de schoolinstellingen neergelegd wenst te worden. Anders dan de reeds bestaande boetes van de AP – een inlogmiddel is immers een persoonsgegeven.* |
| Heeft de aanbieder verantwoordelijkheid geaccepteerd voor het naleven van alle verplichtingen die aan andere partijen zijn uitbesteed? | 2.4.1 | *Besluiten om dit onderdeel te laten zijn van een toetredingsovereenkomst of afspraak binnen de sector.* |
| Heeft de aanbieder bij het uitbesteden aan andere partijen verantwoordelijkheid geaccepteerd voor het voldoen aan het beleid inzake het stelsel voor elektronische identificatie, op dezelfde wijze als wanneer hij deze taken zelf zou vervullen? | 2.4.1 | *Besluiten om dit onderdeel te laten zijn van een toetredingsovereenkomst of afspraak binnen de sector.* |
| Als het stelsel voor elektronische identificatie niet volgens Nederlands recht is opgezet, beschikt het dan over een effectief beëindigingsplan? | 2.4.1 | *Besluiten om dit onderdeel te laten zijn van een toetredingsovereenkomst of afspraak binnen de sector.* |
| Behandelt het beëindigingsplan (1) de ordelijke stopzetting van de dienstverlening dan wel voortzetting door een andere aanbieder, (2) de wijze waarop betrokken autoriteiten en eindgebruikers worden geïnformeerd, en (3) de manier waarop de administratie wordt beschermd, bewaard en vernietigd conform het voor het stelsel voor elektronische identificatie geldende beleid? | 2.4.1 | *Aanname:* als een schoolinstelling sluit, dan zullen leerlingen/studenten op een nieuwe school ingeschreven moeten worden. Dan volgt opnieuw het inschrijfproces? |
| Gepubliceerde mededelingen en informatie voor de gebruikers |  |  |
| Is er een gepubliceerde beschrijving van de dienst met alle toepasselijke voorwaarden en vergoedingen, inclusief eventuele gebruiksbeperkingen? | 2.4.2 | *Controle vraag:* Is de beschrijving incl. eventuele gebruikersbeperkingen van de dienst onderdeel van de gecommuniceerde voorwaarden (zie 2.1.1). En geldt dat ook voor vergoedingen, als die van toepassing is?  **Keuze maken***: of een vergoeding van toepassing is. Kan onderdeel zijn van een toetreding of afspraak binnen de sector.* |
| Bevat de beschrijving ook een privacyverklaring? | 2.4.2 | *Controle vraag:* Is de dienst onderdeel van de privacyverklaring richting leerling/student en medewerker? |
| Zijn er passend beleid en passende procedures om gebruikers van de dienst te informeren over elke wijziging van de dienstbeschrijving, alle toepasselijke voorwaarden en de privacyverklaring? | 2.4.2 | *Controle vraag:*   Worden gebruikers geïnformeerd bij wijziging in de dienstverlening? Bv. door een interne nieuwsbrief of serviceberichten vanuit de ICT-afdeling. |
| Zijn er passend beleid en passende procedures om informatieverzoeken volledig en correct te beantwoorden? | 2.4.2 | *Aanname:* Ja, reeds een verplichting vanuit de AVG |
| Beheer van informatiebeveiliging |  |  |
| Is er een effectief informatiebeveiligingsmanagementsysteem (ISMS) voor het beheer en de beheersing van informatiebeveiligingsrisico’s? | 2.4.3 | *Aanname: veel schoolinstellingen hebben geen volwaardig ISMS ingericht. Wel besteden zij aandacht aan IBP en wordt binnen de sector aangegeven hoe dit ingevuld moet worden met een Toetsingskader IBP.*  **Keuze maken:** of de toepassing van het toetsingskader op een bepaald niveau moet liggen en daarmee voldoende is om aan deze norm te voldoen. |
| Bijhouden van de administratie |  |  |
| Wordt relevante informatie vastgelegd en bewaard met behulp van een doeltreffend documentenbeheersysteem? | 2.4.4 | *Aanname:* Ja, dit wordt standaard opgeslagen in het dossier van de leerling/student en medewerker. Het systeem voor gebruikersbeheer bevat de overige relevante gegevens. |
| Worden hierbij de toepasselijke wetgeving en goede praktijken op het gebied van gegevensbescherming en gegevensbewaring in acht genomen? | 2.4.4 | *Aanname:* Ja, reeds een verplichting vanuit de AVG – naleving van het bewaartermijn.  *Zie ISO 27001 - 18.1.3 Beschermen van registraties*  *Besluiten om dit onderdeel te laten zijn van een toetredingsovereenkomst of afspraak binnen de sector.* |
| Worden de gegevens bewaard zolang het is toegestaan volgens Nederlandse wet- en regelgeving? | 2.4.4 | Zie hierboven. |
| Worden de bewaarde gegevens beschermd zolang zij nodig kunnen zijn voor financiële controle en/of onderzoek van beveiligingsinbreuken? | 2.4.4 | Zie hierboven. |
| Worden de gegevens na afloop van de bewaringstermijn veilig vernietigd? | 2.4.4 | Zie hierboven. |
| Faciliteiten en personeel |  |  |
| Zijn er procedures die waarborgen dat personeelsleden en subcontractanten (1) voldoende zijn opgeleid, (2) voldoende gekwalificeerd zijn en (3) ervaren zijn in de vaardigheden voor de taken die moeten worden vervuld? | 2.4.5 | *Controle vraag*:Zijn de juiste medewerkers – met de juiste vaardigheden - onderdeel van de betrokken processen?  *Zie ISO 27001 - 7.1.1 Screening.* |
| Zijn er voldoende personeelsleden en subcontractanten om de dienstverlening voldoende te waarborgen overeenkomstig het beleid en de procedures? | 2.4.5 | *Besluiten om dit onderdeel te laten zijn van een toetredingsovereenkomst of afspraak binnen de sector.* |
| Staan de gebruikte faciliteiten onder permanente controle en worden zij permanent beschermd tegen schade door milieu-invloeden, ongeoorloofde toegang en andere factoren die de veiligheid van de dienst kunnen aantasten? | 2.4.5 | *Aanname: onderdeel van het Toetsingskader IBP voor het onderwijs.*  *Zie ISO 27001 - 11.1.4 Beschermen tegen bedreigingen van buitenaf* |
| Zijn de gebruikte faciliteiten zo ingericht dat toegang tot zones met persoonsgegevens, cryptografische gegevens en andere gevoelige informatie is beperkt tot bevoegden? | 2.4.5 | *Aanname: onderdeel van het Toetsingskader IBP voor het onderwijs.*  *Zie ISO 27001 - 11.1.1 Fysieke beveiligingszone* |
| Technische controles |  |  |
| Zijn er proportionele controles die gericht zijn op het beheersen van risico’s voor de veiligheid van de dienst(en), waarbij vertrouwelijkheid, integriteit en beschikbaarheid van de informatieverwerking worden beschermd? | 2.4.6 | *Aanname:* onderdeel van het Toetsingskader IBP voor het onderwijs.  *Zie ISO27001 - 18.2.3 Beoordeling van technische naleving* |
| Worden de elektronische communicatiekanalen die voor de uitwisseling van persoonsgegevens en gevoelige gegevens worden gebruikt, beschermd tegen afluisteren, manipuleren en herafspelen? | 2.4.6 | *Controle vraag:* Zijn de communicatiekanalen beveiligd, conform UBV TLS?  *Zie ISO27001 - A.13.2.3 Elektronische berichten* |
| Is de toegang tot gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, beperkt tot de uitoefening van taken en toepassingen waarvoor de toegang strikt noodzakelijk is? | 2.4.6 | *Aanname:* er wordt niet met een crypotgrafisch inlogmiddel gewerkt, maar met een gebruikersnaam en wachtwoord. Het wachtwoord wordt doorgaans gehashed opgeslagen, waarmee deze reeds beschermd zijn.  *Controle vraag:* Wordt het wachtwoord voldoende veilig opgeslagen, zodat het voor niemand toegankelijk is? Zo niet, dan dient de toegang hiertoe beschermd te worden. |
| Wordt de veiligheid procedureel en duurzaam gewaarborgd? | 2.4.6 | *Besluiten om dit onderdeel te laten zijn van een toetredingsovereenkomst of afspraak binnen de sector.* |
| Wordt een respons op wijzigingen van het risiconiveau, incidenten en veiligheidsinbreuken procedureel en duurzaam gewaarborgd? | 2.4.6 | *Aanname:* onderdeel van het Toetsingskader IBP voor het onderwijs.  *Zie ISO27001 - 16.1.5 Respons op informatiebeveiligingsincidenten* |
| Worden alle media die persoonsgegevens, cryptografische informatie of andere gevoelige informatie bevatten, veilig opgeslagen, vervoerd en verwijderd? | 2.4.6 | *Aanname:* onderdeel van het Toetsingskader IBP voor het onderwijs.  *Zie ISO27001 - 8.3.1 Beheer van verwijderbare media* |
| Compliance en audit |  |  |
| Vinden er periodieke interne audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, zodat de naleving van het desbetreffende beleid wordt gewaarborgd? | 2.4.7 | *Controle vraag:* Vindt er een interne audit plaatst op de eisen die gesteld worden voor niveau Laag? |

1. NCS 7516 vormt het certificatieschema voor NTA 7516 – Eisen voor veilige e‐mail en chatapplicaties. Valt onder de NEN Normcommissie 303006 'Informatievoorziening in de zorg' [↑](#footnote-ref-2)
2. https://www.rijksoverheid.nl/onderwerpen/paspoort-en-identiteitskaart/vraag-en-antwoord/wat-is-de-identificatieplicht [↑](#footnote-ref-3)
3. https://www.rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/wat-moet-ik-als-werkgever-doen-om-te-voldoen-aan-de-identificatieplicht [↑](#footnote-ref-4)