Nummer	Tabblad	Cel	Niveau	Reden van verzoek	Tekst oud	Tekst nieuw (voorstel)	Status	Toelichting
2024030	Stap 2.			Alternatief voor aanpassen van de vraag over soort persoonsgegevens; een vraag apart toevoegen voor minderjarige; dat maakt het overzichtelijker. N.a.v. opmerking over minderjarige; die zijn extra kwetsbaar. Zie RFC202404	Geen	Worden er persoonsgegevens verwerkt van minderjarige (leerlingen onder de 16 jaar). Zo ja, welke daarvan worden verwerkt in de toepassing? - Laag = nee, er worden geen persoonsgegevens van minderjarige verwerkt. - Midden = "gewone" persoonsgegevens, zoals adres, enkele toetsresultaten per leerling, inschrijvingsgegevens, etc. - Hoog = Onderwijs- en ontwikkelgegevens, zoals studievoortgang, aanwezigheid en opmerkingen over (gedrag van) leerlingen.	Analyse nodig	Vraag toegevoegd specifiek voor minderjarige, aangezien dit een kwetsbare groep is die beter beschermd moet worden; dus eerder in een hoger niveau moet komen. N.B. Deze vraag toevoegen na de 1e vraag (RFC2024031) over Vertrouwelijkheid, om verwarring te voorkomen bij de invuller.
2024031	Stap 2.			N.a.v. RFC 2024030, dient deze vraag aangepast te worden om tegenstrijdigheid te voorkomen. Daarnaast dient niveau Hoog aangepast te worden met Gevoelige persoonsgegeven, zoals de AP dit ook duidt. Zie https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/wat-zijn-persoonsgegevens#	Welke type persoonsgegevens bevat de ict-toepassing? - Laag = geen of 'gewone' persoonsgegevens zoals NAW - Midden = persoonsgegevens als toetsresultaten of gegevens m.b.t. minderjarigen. - Hoog = bijzondere persoonsgegevens, zoals gegevens over etniciteit, politieke opvatting, geloof, gezondheid, seksueel gedrag, etc.	Welke type persoonsgegevens bevat de toepassing? - Laag = geen of 'gewone' persoonsgegevens zoals NAW - Midden = Onderwijs- en ontwikkelgegevens, zoals studievoortgang, aanwezigheid en opmerkingen over leerlingen. - Hoog = Gevoelige persoonsgegevens zoals een kopie ID, Burgerservicenummer (BSN), gegevens over locatie en inkomen, en bijzondere categorieën van persoonsgegevens (bijv. gezondheidsgegevens, genetische en biometrische gegevens, politieke opvattingen, religieuze overtuigingen, etc.).	Analyse nodig	Antwoorden Midden en Hoog aangepast. - Midden aangepast naar Onderwijs- en ontwikkelgegevens. - Hoog uitgebreid met Gevoelige persoonsgegevens met voorbeelden (o.b.v. de AP).
2024007a	Beschikbaarheid	H6	Midden	Onduidelijk wat er exact verwacht wordt en het toesturen van verzwarende cijfers is inherent niet een verzwarende maatregel	Terwijl de toepassing wordt gebruikt, wordt de beschikbaarheid van de toepassing en aanpalende toepassingen gemonitord. Naar aanleiding van deze monitoring wordt bij uitval een gestructureerd proces gestart voor notificatie en herstel van de keten.	Terwijl de toepassing wordt gebruikt, wordt de **huidige** beschikbaarheid van de toepassing en aanpalende toepassingen gemonitord. Naar aanleiding van deze monitoring wordt bij uitval een gestructureerd proces gestart voor notificatie aan de afnemer en herstel van de keten. **De recente beschikbaarheid is opvraagbaar door de afnemer.**	Voorleggen	Expliciet gemaakt waar we huidige en recente beschikbaarheid bedoelen. De 1e en 2e alinea is bijgewerkt dat het om de huidige beschikbaarheid gaat, dat gemeld moet worden aan de afnemer. In de 3e alinea is duidelijk gemaakt dat de historie opvraagbaar is, i.p.v. proactief bij
2024007b	Beschikbaarheid	H7	Hoog	Onduidelijk wat er exact verwacht wordt en het toesturen van verzwarende cijfers is inherent niet een verzwarende maatregel	Terwijl de toepassing wordt gebruikt, wordt de beschikbaarheid van de toepassing en aanpalende toepassingen gemonitord. Naar aanleiding van deze monitoring wordt bij uitval een gestructureerd proces gestart voor notificatie en herstel van de keten. De cijfers van de recente en huidige beschikbaarheid van de toepassing zijn opvraagbaar voor belanghebbenden.	Terwijl de toepassing wordt gebruikt, wordt de **huidige** beschikbaarheid van de toepassing en aanpalende toepassingen gemonitord. Naar aanleiding van deze monitoring wordt bij uitval een gestructureerd proces gestart voor notificatie **aan de afnemer** en herstel van de keten. **De recente beschikbaarheid wordt proactief gerapporteerd (bijvoorbeeld via een portaal of servicegesprek) aan de afnemer.**	Voorleggen	Expliciet gemaakt waar we huidige en recente beschikbaarheid bedoelen. In de 1e en 2e alinea is bijgewerkt dat het om de huidige beschikbaarheid gaat, dat gemeld moet worden aan de afnemer. In de 3e alinea is duidelijk gemaakt dat de recente beschikbaarheid gerapporteerd moeten worden.
2024009	Integriteit	F7	Hoog	Onduidelijk wat het verschil is tussen midden en hoog is. Geen verschil tussen midden en hoog	Controle op invoer/uitvoer en andere methoden van wijzigen van gegevens: - De toepassing controleert invoer (handmatig of via geautomatiseerde koppeling) door bijvoorbeeld syntax-controle en controle op verplichte velden. In geval van een uploadfunctie, wordt deze beperkt en bestanden worden gecontroleerd. - Uitvoer naar andere systemen wordt opgeschoond tot (veilige) waardes, bv. op basis van syntax-controle. - Foutmeldingen voor gebruikers zijn beperkt; niet meer tonen dan nodig. - Wijzigingen 'onder water' (zonder gebruik van de gebruikersinterface) worden als beveiligingsincident opgemerkt en afgehandeld	Controle op invoer/uitvoer en andere methoden van wijzigen van gegevens: - De applicatie controleert de ingevoerde gegevens (handmatig of via geautomatiseerde koppeling) op syntax, verplichte velden **en integriteit (bv. met hashing)**. - In geval van een uploadfunctie, wordt deze beperkt en bestanden worden gecontroleerd. - Uitvoer naar andere systemen wordt opgeschoond tot (veilige) waardes, bv. op basis van syntax-controle. - Foutmeldingen voor gebruikers zijn beperkt; niet meer tonen dan nodig. - Wijzigingen 'onder water' (zonder gebruik van de gebruikersinterface) worden als beveiligingsincident opgemerkt en	Voorleggen	Er hoeft geen verschil te zijn. N.a.v. deze opmerking wel: regel toegevoegd voor hashing bij koppeling tussen systemen. Na besluit van de werkgroep (17-9-2024) is de wijziging herzien. We houden het bij de functionele beschrijving, die reeds gevangen wordt onder de 1e bullet. Wel hebben we hashing als voorbeeld meegenomen, om extra duiding te geven.
2024013	Vertrouwelijkheid	E6	Midden	Bij 'hoog' is vanuit het ROSA certificeringsschema, een 2FA verplicht is voor alle gebruikers van het systeem maar behoeft niet te zijn voor leerlingen	De toepassing ondersteunt minimaal de volgende maatregelen: - Twee-factor authenticatie (gebruikersnaam en wachtwoord aangevuld met bijvoorbeeld een code op een mobiele telefoon, token of machine certificaat), minimaal voor alle beheerders van de toepassing - Accounts zijn persoonlijk identificeerbaar - Wachtwoordeisen die voldoen aan best practices zoals de richtlijnen van NIST* Er is een geïmplementeerd beleid voor logische toegang (zoals voor supportmedewerkers, beheerders, ontwikkelaars etc.). Daarin zit minimaal een periodieke controle actieve accounts versus actieve medewerkers. En zijn bovenstaande maatregelen van toepassing.	De toepassing ondersteunt minimaal de volgende maatregelen: - Twee-factor authenticatie (2FA) en wordt **standaard** afgedwongen voor **alle gebruikers behalve leerlingen**. - Bij federatieve inlog neemt de toepassing de 2FA van de authenticatiedienst over. Als dit niet mogelijk is, wordt de eigen 2FA afgedwongen. - Accounts zijn persoonlijk identificeerbaar - Wachtwoordeisen die voldoen aan best practices zoals de richtlijnen van NIST* Er is een geïmplementeerd beleid voor logische toegang (zoals voor supportmedewerkers, beheerders, ontwikkelaars etc.). Daarin zit minimaal een periodieke controle actieve accounts versus actieve medewerkers. En zijn bovenstaande maatregelen van toepassing.	Voorleggen	Niveau Midden verzwaard: niet alleen beheerders, maar ook docenten en leraren die toegang hebben tot anderemans persoonsgegevens. Ofwel, iedereen behalve de leerling zelf. Aangezien applicaties nu eerder in Hoog geplaatst worden - door aanpassing van de BIV-vragen - is deze verzwaring voldoende. N.B. Voor Hoog geldt 2FA voor iedereen.

2024033	Vertrouwelijkheid	B7	Hoog	In de vragen hebben we gevoelige gegevens geïntroduceerd, maar deze komt nog niet terug in de definitie van Geheim.	Informatie is geheim. De organisatie, instelling of betrokkene kan ernstige schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag uitsluitend toegankelijk zijn voor een zeer geselecteerde groep personen. Hieronder vallen onder andere bijzondere persoonsgegevens.	Informatie is geheim. De organisatie, instelling of betrokkene kan ernstige schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag uitsluitend toegankelijk zijn voor een zeer geselecteerde groep personen. Hieronder vallen onder andere gevoelige persoonsgegevens, waaronder bijzondere persoonsgegevens	Analyse nodig	Naast bijzondere persoonsgegevens worden ook gevoelige persoonsgegevens genoemd, zoals nu ook in Stap 2. wordt benoemd.
2024035a	Beschikbaarheid	F6	Laag	De maatregel gaat over onderhoud, zoals updates doorvoeren. Het zou niet om frequentie moeten gaan, maar de geplandheid om gebruikersimpact te verkleinen conform de beschikbaarheidseisen.	Security patches, updates (firmware en software) en vernieuwing van certificaten worden ad hoc uitgevoerd. Urgente security patches worden zo spoedig mogelijk doorgevoerd. Software van derden (zoals operating system of libraries) moet actief onderhouden zijn; mag niet End-of-Support zijn.	Onderhoud (zoals updates, security patches en certificaatvernieuwingen) vindt plaats. Hoge en kritieke security patches worden direct beoordeeld voor eigen situatie en zo snel als redelijkerwijs mogelijk doorgevoerd. Software van derden (zoals operating system of libraries) moet actief onderhouden zijn; mag niet End-of-Support zijn.	Voorleggen	1e alinea begonnen met Onderhoud, aangezien het daarom gaat om beschikbaarheid te waarborgen. Daarnaast (n.a.v. 2024035b) verduidelijkt dat het om Hoge en Kritieke security patches gaat.
2024035b	Beschikbaarheid	F6	Midden	Urgente Security patches is niet duidelijk genoeg.	Security patches, updates (firmware en software) en vernieuwing van certificaten worden met vaste regelmaat in de toepassing uitgevoerd, bijvoorbeeld middels een maandelijks of geautomatiseerd proces. Urgente security patches worden direct beoordeeld en zo snel als redelijkerwijs doorgevoerd. Software van derden (zoals operating system of libraries) moet actief onderhouden zijn; mag niet End-of-Support zijn.	Onderhoud (zoals updates, security patches en certificaatvernieuwingen) vindt gepland plaats. Een rollback-scenario is beschikbaar. Hoge en kritieke security patches worden direct beoordeeld voor eigen situatie en zo snel mogelijk doorgevoerd. Software van derden (zoals operating system of libraries) moet actief onderhouden zijn; mag niet End-of-Support zijn.	Voorleggen	Urgente kwetsbaarheden veranderd naar Hoge en Kritieke conform CVSS classficatie. Daarnaast (n.a.v. 2024035a) 1e alinea aangepast: Gepland en met rollback-scenario.
2024036	Beschikbaarheid	F7	Hoog	zie 2024036	Security patches, updates (firmware en software) en vernieuwing van certificaten worden met vaste regelmaat in de toepassing uitgevoerd, bijvoorbeeld middels een maandelijks of geautomatiseerd proces. Urgente security patches worden direct beoordeeld en zo snel als redelijkerwijs doorgevoerd. Er wordt – waar mogelijk – geautomatiseerd gecontroleerd op security-gerelateerde patches en updates. Software van derden (zoals operating system of libraries) moet actief onderhouden zijn; mag niet End-of-Support zijn.	Onderhoud (zoals updates, security patches en certificaatvernieuwingen) vindt tijdens afgesproken onderhoudswindows plaats. Een rollback-scenario is beschikbaar. Hoge en kritieke security patches worden direct beoordeeld voor eigen situatie en zo snel mogelijk doorgevoerd. Software van derden (zoals operating system of libraries) moet actief onderhouden zijn; mag niet End-of-Support zijn.	Voorleggen	N.a.v. 2024035 dient hier de tekst ook aangepast worden. Urgente veranderd naar Hoge en Kritieke conform CVSS classficatie Daarnaast automatische controle van patches hier verwijderd, aangezien dit eerder thuis hoort bij omgaan met kwetsbaarheden onder Vertrouwelijkheid (is verwerkt met RFC 2024044c).
2024011	Integriteit	I6	Midden	Onduidelijk met welke frequentie dit gedaan moet worden	Periodieke controle integriteit toepassing: - De status van doorgevoerde patches en updates van firmware en software worden periodiek gecontroleerd - Integriteit van de configuratie en software wordt structureel gecontroleerd door een regelmatig uitgevoerd proces Maatregelen tegen malware zijn toegepast Secure software development/secure coding guidelines worden toegepast	Periodieke controle integriteit toepassing: - De status van patches en updates van firmware en software wordt periodiek (minimaal jaarlijks) gecontroleerd. - De integriteit van configuratie en software wordt structureel gecontroleerd, minimaal na elke wijziging/update en anders minimaal jaarlijks. Maatregelen tegen malware zijn toegepast Secure software development/secure coding guidelines worden toegepast	Voorleggen	Frequentie van minimaal jaarlijks verwerkt in de tekst en tekst hierop aangepast.
2024037	Integriteit	G5	Laag	Het is niet duidelijk door wie de logging gecontroleerd moet worden.	Gelogd wordt: inlogactiviteit gebruikers. Deze logging wordt alleen gebruikt voor controle of ondersteuning (doelbinding) en minimaal 13 maanden bewaard, tenzij expliciet anders is afgesproken. Voor de kwaliteit van logging worden best practices overwogen (bijvoorbeeld OWASP Logging cheat sheet) Logging wordt ad hoc gecontroleerd (bijvoorbeeld bij incidenten)	Functionele logging: wordt niet geeïst.	Voorleggen	Inlog activiteit wordt al geeist onder vertrouwelijkheid. Kan hier dus weg. Het gaat hier om functionele logging.
2024038	Integriteit	G6	Midden	Het is niet duidelijk door wie de logging gecontroleerd moet worden.	Gelogd wordt: inlogactiviteit gebruikers en wijziging van (persoons)gegevens. Deze logging wordt alleen gebruikt voor controle of ondersteuning (doelbinding) en minimaal 13 maanden bewaard, tenzij expliciet anders is afgesproken. Voor de kwaliteit van logging worden best practices gehanteerd (bijvoorbeeld OWASP Logging cheat sheet) Logging wordt periodiek gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera)	Functionele logging: wijziging van (persoons)gegevens wordt gelogd. Deze logging is minimaal 13 maanden beschikbaar voor controle op afwijkende patronen (frequentie, oorsprong, et cetera) en ondersteuning. Logging is alleen toegankelijk voor geautoriseerde medewerkers en wordt beschermd tegen wijzigingen.	Voorleggen	Wie welke logging moet controleren, wordt bepaald door de soort logging. Hier gaat het om functionele logging, die door de gebruiker zelf gecontroleerd kan worden. Hierdoor kunnen beide partijen (afnemer en leveranciers) afwijkingen patronen signaleren. Verder tekstuele aanscherpingen. Kwaliteit van logging wordt al genoemd bij een andere maatregel.

2024039	Integriteit	G7	Hoog	Het is niet duidelijk door wie de logging gecontroleerd moet worden.	Gelogd wordt: inlogactiviteit gebruikers en wijziging van (persoons)gegevens. Deze logging wordt alleen gebruikt voor controle of ondersteuning (doelbinding) en minimaal 13 maanden bewaard, tenzij expliciet anders is afgesproken. Voor de kwaliteit van logging worden best practices gehanteerd (bijvoorbeeld OWASP Logging cheat sheet) Logging wordt geautomatiseerd gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera) Logging is alleen toegankelijk voor relevante medewerkers en wordt beschermd tegen ongeautoriseerde wijzigingen.	Functionele logging: wijziging van (persoons)gegevens wordt gelogd. Deze logging is minimaal 13 maanden beschikbaar voor controle op afwijkende patronen (frequentie, oorsprong, et cetera) en ondersteuning. Deze controle vindt automatisch plaats. Logging is alleen toegankelijk voor geautoriseerde medewerkers en wordt beschermd tegen wijzigingen.	Voorleggen	Wie welke logging moet controleren, wordt bepaald door de soort logging. Hier gaat het om functionele logging, die door de gebruiker zelf gecontroleerd kan worden. Hierdoor kunnen beide partijen (afnemer en leveranciers) hun verantwoordelijkheden nemen. Voor dit niveau geldt dat de controle automatisch plaatsvindt. Verder tekstuele aanscherpingen. Kwaliteit van logging wordt al genoemd bij een andere maatregel.
2024034	Stap 2.	H15			Past de toepassing profilering* toe? - Laag = nee - Midden = ja, maar deze leidt niet tot automatische beslissingen (alleen handmatig) - Hoog = ja, en deze leidt tot automatische beslissingen (door de toepassing zelf)	Past de toepassing profilering* toe? - Laag = nee - Midden = ja, maar deze leidt niet tot automatische beslissingen (alleen handmatig) of hebben geen impact voor de betrokkene - Hoog = ja, en deze leidt tot automatische beslissingen (door de toepassing zelf) met een aanzienlijke impact voor de betrokkene	Analyse nodig	Willen we deze anders ook meenemen in het advies van het KAP? Ja!
2024041	Stap 2.	M13		Ik mis daar dan de volgende aspecten in: Reputatie- en andersoortige schade als gevolg van inbreuk op vertrouwelijkheid (kennisveiligheid bijvoorbeeld).	Leidt het uitlekken van de gegevens tot economische schade? - Laag = nee - Midden = beperkte economische schade - Hoog = aanzienlijke economische schade	Leidt het uitlekken van de gegevens tot economische, reputatie- of andersoortige schade? - Laag = geen economische of reputatieschade - Midden = beperkte economische en/of reputatieschade - Hoog = aanzienlijke economische en/of reputatieschade, inclusief inbreuk op kennisveiligheid	Voorleggen	Voorstel ziet in behoefte.
2024020	Stap 4.	B2		Het is **niet** verplicht om controls waar je aan voldoet te motiveren/onderbouwen	Hieronder staan de maatregelen die van toepassing zijn op basis van de BIV-classificatie van de ict-toepassing. Selecteer per maatregel wat hier de status van is. Bij niet voldaan: geef aan hoe/wanneer dit wordt gecorrigeerd. Bij alternatieve maatregel: beschrijven deze. Hetgeen geselecteerd en beschreven wordt meegenomen in de rapportage (volgende tabblad).	De onderstaande maatregelen zijn van toepassing op basis van de BIV-classificatie. Selecteer per maatregel de huidige status en geef bij 'niet voldaan' aan hoe en wanneer dit wordt gecorrigeerd. Wanneer een alternatieve maatregel is genomen, beschrijf deze dan. De geselecteerde statussen en beschrijvingen worden meegenomen in de rapportage op het volgende tabblad. N.B. Bij de status Voldoet is het niet verplicht om in detail te beschrijven hoe deze is geïmplementeerd. Wel wordt aangeraden om dit in te vullen, zodat de informatie eenvoudig beschikbaar is wanneer hierom wordt gevraagd. Het aanleveren van deze informatie kan verplicht zijn, bijvoorbeeld in het kader van een DPIA of het meewerken aan een audit van opdrachtgever. **Let op! Excelfunctie bijwerken, zodat omschrijving niet meegenomen worden als status = Voldoet**	Voorleggen	Het is niet gewenst om deze wijze van implementatie standaard transparant te maken. Dit is alleen relevant als je niet voldoet of de maatregel elders hebt ingevul, zoals het nu verplicht is. Als meer informatie nodig is, kan dit opgevraagd worden bij de leverancier. Dit dient ook geleverd te worden in bv. in het kader van right to audit of het meewerken aan DPIA's. Op basis hiervan de tekst verduidelijkt.
2024014	Vertrouwelijkheid	I7	Hoog	Encryptie van opslag, moet minimaal op twee niveaus, zoals op (virtuele)disk en bestands- of recordniveau. Deze wordt als niet realistisch ervaren bij leveranciers. Graag bespreken aan de hand van de motivering van een leverancier.	Encryptie van transport (zowel voor intern als extern verkeer) is conform de Uniforme Beveiligingsvoorschriften (UBV) TLS van Edustandaard. Encryptie van opslag, moet minimaal op twee niveaus, zoals op (virtuele)disk en bestands- of recordniveau. Hiervoor wordt gebruik gemaakt van richtlijnen/best practices/standaarden, zoals van NCSC, ENISA, NIST.	Encryptie van transport (zowel voor intern als extern verkeer) is conform de Uniforme Beveiligingsvoorschriften (UBV) TLS van Edustandaard. Encryptie van opslag, moet minimaal op twee niveaus, zoals op disk (ter beveiliging bij fysieke diefstal) en bestands- of recordniveau (ter beveiliging bij exfiltratie). Hiervoor wordt gebruik gemaakt van richtlijnen/best practices/standaarden, zoals van NCSC, ENISA, NIST.	Voorleggen	Bezwaren worden niet door iedereen gedeeld in de werksessie. Encryptie op applicatieniveau, kan op verschillende manieren, zonder dat in de weg hoeft te zitten voor het gebruik. Dit wordt anders als het op gebruikersnvieau wordt versleuteld. N.B. Tekst is verder verduidelijkt met het aangeven van de reden.
2024017	Vertrouwelijkheid	E7	Hoog	Onduidelijk welke extra maatregelen genomen moeten worden bij Hoog ten opzichte van Midden	De toepassing ondersteunt minimaal de volgende maatregelen: - Twee-factor authenticatie (gebruikersnaam en wachtwoord aangevuld met bijvoorbeeld een code op een mobiele telefoon, token of machine certificaat) voor alle gebruikers van de toepassing - Accounts zijn persoonlijk identificeerbaar - Wachtwoordeisen die voldoen aan best practices zoals de richtlijnen van NIST* Er is een geïmplementeerd beleid voor logische toegang (zoals voor supportmedewerkers, beheerders, ontwikkelaars etc.). Daarin zit minimaal een periodieke controle actieve accounts versus actieve medewerkers. En zijn bovenstaande maatregelen van toepassing.	De toepassing ondersteunt minimaal de volgende maatregelen: - Twee-factor authenticatie (2FA) en wordt **standaard** afgedwongen voor **alle gebruikers**. - Bij federatieve inlog neemt de toepassing de 2FA van de authenticatiedienst over. Als dit niet mogelijk is, wordt de eigen 2FA afgedwongen. - Accounts zijn persoonlijk identificeerbaar - Wachtwoordeisen die voldoen aan best practices zoals de richtlijnen van NIST* Er is een geïmplementeerd beleid voor logische toegang (zoals voor supportmedewerkers, beheerders, ontwikkelaars etc.). Daarin zit minimaal een periodieke controle actieve accounts versus actieve medewerkers. En zijn bovenstaande maatregelen van toepassing.	Voorleggen	Midden is al aangescherpt, zie regel 2024013. Deze maatregel is in lijn gebracht met het lagere niveau, echter geldt 2FA op dit niveau voor alle gebruikers.

2024027	Vertrouwelijkheid	H7	Hoog	Maatregel is niet afdoende, voldoet niet aan best practices	Ontwikkel, test, acceptatie en productieomgevingen (OTAP) zijn gescheiden. Productiedata (persoonsgegevens, gebruikersnamen, wachtwoorden, et cetera) worden uitsluitend geanonimiseerd gebruikt in ontwikkel- en testomgevingen en waar mogelijk ook in de acceptatieomgevingen. Toegang tot OTAP wordt beheerd en periodiek gecontroleerd en geeft invulling aan de principes ‘need to know’ en ‘least privilege’. Bijvoorbeeld: ontwikkelaars hebben niet standaard toegang tot productieomgevingen. Daarnaast hebben gebruikers standaard geen toegang tot OTA.	Ontwikkel, test, acceptatie en productieomgevingen (OTAP) zijn gescheiden. Productiedata (persoonsgegevens, gebruikersnamen, wachtwoorden, et cetera) wordt niet gebruikt in OTA. **Bij voorkeur wordt dummy data gebruikt en anders niet-herleidbaar (geanonimiseerd).** Toegang tot OTAP wordt beheerd en periodiek gecontroleerd en geeft invulling aan de principes ‘need to know’ en ‘least privilege’. Bijvoorbeeld: ontwikkelaars hebben niet standaard toegang tot productieomgevingen. Daarnaast hebben gebruikers standaard geen toegang tot OTA.	Voorleggen	Best-practices is om geen productiedata anoniem te gebruiken, maar gebruik temaken van dummy data. Annonimiseren is lastiger dan dummy data creeëren met bv.AI
2024042a	Vertrouwelijkheid	G5	Laag	wat betekent de laatste bullet? wat is extern benaderbaar? Niet de diensten zelf namelijk, die staan immers publiek op het internet. Let op! dit geldt voor elk niveau.	Er is een geïmplementeerd beleid voor netwerktoegang. Daarin zitten minimaal de volgende maatregelen: - Netwerksegmentatie, bijvoorbeeld door middel van VLANs - Toegang vanuit andere zones is beschermd met aanvullende maatregelen zoals een firewall die poorten dichtzet en geoblocking toepast - Extern benaderbaar door medewerkers en beheerders alleen via beveiligde verbinding met authenticatie en encryptie	Er is een geïmplementeerd beleid voor netwerktoegang. Daarin zitten minimaal de volgende maatregelen: - Netwerkzones voor beheer, servers en gebruikers zijn van elkaar gescheiden, bijvoorbeeld met VLANs. - Toegang tussen netwerkzones is beperkt met basismaatregelen en alleen noodzakelijke poorten staan open. - Toegang vanaf het internet is beperkt tot gebruikerstoegang en alleen vanuit noodzakelijke landen; overige landen zijn standaard geblokkeerd (geoblocking). - Beheertoegang is alleen mogelijk via een beveiligde verbinding (bv. VPN) met 2FA.	Voorleggen	Een toepassing is tegenwoordig altijd extern te benaderen. Het zou hier om beheertoegang moeten gaan. Deze dient via een beveiligde verbinding te verlopen.
2024042b	Vertrouwelijkheid	G6	Midden	Zie 2024042a	Er is een geïmplementeerd beleid voor netwerktoegang. Daarin zitten minimaal de volgende maatregelen: - Netwerksegmentatie, bijvoorbeeld door middel van VLANs - Toegang vanuit andere zones is beschermd met aanvullende maatregelen zoals een firewall die poorten dichtzet en geoblocking toepast - Extern benaderbaar door medewerkers en beheerders alleen via beveiligde verbinding met authenticatie en encryptie	Er is een geïmplementeerd beleid voor netwerktoegang. Daarin zitten minimaal de volgende maatregelen: - Netwerkzones voor beheer, servers en gebruikers zijn van elkaar gescheiden, bijvoorbeeld met VLANs. - Toegang tussen netwerkzones is beperkt met basismaatregelen en alleen noodzakelijke poorten staan open. - Toegang vanaf het internet is beperkt tot gebruikerstoegang en alleen vanuit noodzakelijke landen; overige landen zijn standaard geblokkeerd (geoblocking). - Beheertoegang is alleen mogelijk **met een jump server** via een beveiligde verbinding (bv. VPN) met 2FA.	Voorleggen	Zie 2024042a. Aanvullend voor dit niveau geldt dat toegang via een steppingstone moet plaatsvinden. N.B. Dikgedrukt geeft aan wat het verschil is met het lagere niveau.
2024042c	Vertrouwelijkheid	G7	Hoog	Zie 2024042a	Er is een geïmplementeerd beleid voor netwerktoegang. Daarin zitten minimaal de volgende maatregelen: - Netwerksegmentatie, bijvoorbeeld door middel van VLANs - Toegang vanuit andere zones is beschermd met aanvullende maatregelen zoals een firewall die poorten dichtzet en whitelisting van IP-adressen - Extern benaderbaar door medewerkers en beheerders alleen via beveiligde verbinding met authenticatie en encryptie	Er is een geïmplementeerd beleid voor netwerktoegang. Daarin zitten minimaal de volgende maatregelen: - Netwerkzones voor beheer, servers en gebruikers zijn van elkaar gescheiden, bijvoorbeeld met VLANs. **Elke toepassing heeft een eigen netwerk, met gescheiden front-end en back-end.** - Toegang tussen netwerkzones is beperkt met basismaatregelen en alleen noodzakelijke poorten staan open. - Toegang vanaf het internet is beperkt tot gebruikerstoegang en alleen vanuit noodzakelijke landen; overige landen zijn standaard geblokkeerd (geoblocking). - Beheertoegang is alleen mogelijk met een *jump server* via een beveiligde verbinding (bv. VPN) met 2FA.	Voorleggen	Zie 2024042a. Aanvullend voor dit niveau geldt elke toepassing zijn eigen netwerk heeft, met gescheiden front-end en back-end. Op volgende bullet geldt dan ook voor deze netwerken; enkel poorten open tussen front-end en back-end die nodig zijn. N.B. Dikgedrukt geeft aan wat het verschil is met het lagere niveau.
2024043	Vertrouwelijkheid	H7	Hoog	Vanuit het Normenkader IBP voor het onderwijs wordt Screening vereist bij leveranciers (HR.01). Dit wordt nu alleen niet vereist vanuit dit schema. Is relevant indien medewerkers toegang hebben tot productiegegevens, zoals adresgegevens van leerlingen.		**Aanvullend toevoegen:** Alle medewerkers die in aanraking kunnen komen met productiegegevens, dienen periodiek (minimaal eens per 5 jaar) gescreend te worden met minimaal een VOG met de juiste categorieën (bv. 01 Informatie).	Voorleggen	Zie reden verzoek. Om hier invulling aan te geven, zouden medewerkers gescreend moeten worden. Echter wel alleen die toegang hebben tot productiegegevens, want dat is de achterliggende gedachten van deze maatregel.

2024044a	Vertrouwelijkheid	K5	Laag	Voor een applicatie met het niveau laag wordt al een risico/dreigingsanalyse vereist. Dit is te zwaar voor een de applicaties die hier onder vallen. Daarmee zouden de opvolgende niveau's ook aangepast moeten worden.	Een risico/dreigingsanalyse zijn uitgevoerd op de toepassing, ter illustratie: - Privacy by design wordt toegepast - OWASP Top 10	De toepassing voldoet aan de Uniforme Beveiligingsvoorschriften (UBV) van Edustandaard. Bekende kwetsbaarheden worden opgevolgd op basis van beveiligingsadviezen (bijv. NCSC). Indien patches ontbreken, worden alternatieve maatregelen genomen.	Voorleggen	In de basis moeten toepassingen voldoen aan de richtlijnen UBV. Daarnaast zouden bekende kwetsbaarheden altijd opgevold moeten worden.
2024044b	Vertrouwelijkheid	K6	Midden	Zie 2024044a	Een risico/dreigingsanalyse zijn uitgevoerd op de toepassing, ter illustratie: - Privacy by design wordt toegepast - Threat modelling - OWASP Top 10 De toepassing wordt getoetst tegen richtlijnen zoals de Uniforme Beveiligingsvoorschriften (UBV) van edustandaard en de NCSC richtlijnen voor webapplicaties. Bekende kwetsbaarheden worden adequate opgevolgd (zoals met NCSC beveiligingsadviezen). Indien patches niet aanwezig zijn, worden er alternatieve maatregelen genomen.	De toepassing voldoet aan de Uniforme Beveiligingsvoorschriften (UBV) van Edustandaard. Bekende kwetsbaarheden worden opgevolgd en op basis van beveiligingsadviezen (bijv. NCSC). Indien patches ontbreken, worden alternatieve maatregelen genomen. **Privacy by design en security by design worden toegepast om kwetsbaarheden zoveel mogelijk te voorkomen. Minimaal jaarlijks of bij grote wijzigingen wordt:** **- Getoetst op veelvoorkomende kwetsbaarheden, zoals de OWASP Top 10 (Privacy Risks), door middel van assessments of geautomatiseerde tests.**	Voorleggen	Aangezien het op dit niveau gaat over vertrouwelijke gegevens, waaronder persoonsgegevens, is privacy- en security by design verplicht/noodzakelijk incl het toetsen daarop met assessments of automatische testen. N.B. Dikgedrukt geeft aan wat het verschil is met het lagere niveau.
2024044c	Vertrouwelijkheid	K7	Hoog	Zie 2024044a	Een risico/dreigingsanalyse zijn uitgevoerd op de toepassing, ter illustratie: - Privacy by design en security by design wordt toegepast - Threat modelling - OWASP Top 10 De toepassing wordt getoetst tegen richtlijnen zoals de Uniforme Beveiligingsvoorschriften (UBV) van edustandaard en de NCSC richtlijnen voor webapplicaties. De toepassing wordt periodiek getoetst op passende bescherming van vertrouwelijkheid (minimaal jaarlijks en bij grote wijzigingen), bijvoorbeeld: - Security testen - Vulnerability testen - Pentesten, onafhankelijk door een externe partij Bekende kwetsbaarheden worden adequate opgevolgd (zoals met NCSC beveiligingsadviezen). Indien patches niet aanwezig zijn, worden er alternatieve maatregelen genomen. Inbraakdetectie- en preventiesystemen (IDS/IPS) zijn aanwezig, om aanvallen te detecteren en waar mogelijk automatisch te blokkeren.	De toepassing voldoet aan de Uniforme Beveiligingsvoorschriften (UBV) van Edustandaard. Bekende kwetsbaarheden worden **automatisch gesignaleerd en** adequaat opgevolgd op basis van beveiligingsadviezen (bijv. NCSC). Indien patches ontbreken, worden alternatieve maatregelen genomen. Privacy by design en security by design worden toegepast om kwetsbaarheden zoveel mogelijk te voorkomen. Minimaal jaarlijks of bij grote wijzigingen wordt: - Getoetst op veelvoorkomende kwetsbaarheden, zoals de OWASP Top 10 (Privacy Risks), door middel van assessments of geautomatiseerde tests. **- een risicoanalyse uitgevoerd (zoals threat modelling) om kwetsbaarheden en dreigingen in kaart te brengen. Voor passende maatregelen wordt aansluiting gezocht bij relevante richtlijnen, zoals die van het NCSC.** **Misbruik van kwetsbaarheden - zoals ongeautoriseerde toegang - wordt gemonitord, herkend en geblokkeerd, zoals met EDR voor het detecteren en mitigeren van verdachte activiteiten.**	Voorleggen	Voor dit niveau geldt meer diepgang, dus een risicoanalyse toegevoegd. Daarnaast detectie van misbruik van kwetsbaarheden. N.a.v. 2024036 is automatisch controleren van patches nu verwerkt in de 2e alinea.