Nummer	Tabblad	Cel	Niveau	Reden van verzoek	Tekst oud	Tekst nieuw (voorstel)	Status	Toelichting
2024023	Inleiding			ISO27001 moet bij X classificatie verplicht worden gesteld, met de juiste scope		ISO27001 verplicht stellen bij bepaald niveau.	Elders behandelen	Meenemen in onderdeel Toezicht, want wel kunnen wel eisen stellen aan de onafhankelijkheid bij een hoge classificatie.
2024024	Inleiding			het is **niet** verplicht om mee te werken aan ROSA		leveranciers verplichten om aan ROSA mee te doen. Nu vaak nog discussiepunt	Elders behandelen	Meenemen in onderdeel Toezicht.
2024025	Inleiding			Onduidelijk wie verantwoordelijk is om ROSA van de leverancier(s) jaarlijks te herzien		volgens toetsingskader dient jaarlijks een review op ROSA plaats te vinden. Dit wordt niet gedaan. Wie bewaakt dit?	Elders behandelen	Dit zou een onderwerp voor onderdeel 'Toezicht' kunnen zijn.
2024002	Inleiding			Classificatie niet laten vaststellen door leverancier maar direct of indirect via schoolbesturen. Mogelijk via FORA.			Elders behandelen	Staat los van het instrument zelf; kan door zowel afnemer als leverancier gebruikt worden. Dit dient elders behandeld te worden: onder het thema BIV-classificatie
2024003	Stap 2.	M9	Midden	Is Hoog categorie omdat het om kwetsbare groepen/ minderjarigen gaat (AVG eis). Tevens ter onderbouwing: zie onderdeel 15 van de verplichte DPIA lijst van de AP. De term' profilering' ziet ook op prestaties van leerlingen. Indien derhalve over een langere periode toetsresultaten/cijfers/voortgang e.d. zijn opgenomen in een applicatie is er sprake van een 'hoog risico' verwerking. Dit leidt tot de conclusie 'Hoog' in plaats van 'Midden'.	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 ict-toepassing? - Laag = geen of 'gewone' persoonsgegevens zoals NAW - Midden = persoonsgegevens die weinig of geen relevantie informatie geven over de leerling (denk aan: klas, leergang, vakkenpakket). - Hoog = bijzondere persoonsgegevens, zoals gegevens over etniciteit, politieke opvatting, geloof, gezondheid, seksueel gedrag, etc. Maar ook persoonsgegevens die vallen onder de definitie van profilering, waaronder het vastleggen van leerprestaties (toetsresultaten, cijfers etc.).	Vervalt	In de werksessie van 22 mei 2024 een alternatief besproken hierop; een extra vraag voor minderjarige, zie 2024030
2024004	Stap 2.	M12	Midden	AVG labelt deze hoog als het om minderjarige/kwetsbare groepen gaat. Tevens ter onderbouwing: zie onderdeel 15 van de verplichte DPIA lijst van de AP. De term' profilering' ziet ook op prestaties van leerlingen. Indien derhalve over een langere periode toetsresultaten/cijfers/voortgang e.d. zijn opgenomen in een applicatie is er sprake van een 'hoog risico' verwerking. Dit leidt tot de conclusie 'Hoog' in plaats van 'Midden'.	Past de toepassing profilering* toe? - Laag = nee - Midden = ja, maar het profiel wordt niet opgeslagen/kan niet opgevraagd worden - Hoog = ja, en het profiel wordt opgeslagen/is inzichtelijk	Wijzigen naar hoog	Vervalt	In de werksessie van 22 mei 2024 een alternatief besproken hierop; een extra vraag voor minderjarige, zie 2024030
2024021	Stap 2.	B3		Het is **niet** verplicht om de classificatie te motiveren. Tijdens bespreken in de werksessie, besloten om de tekst "(indien gewenst)" weg te halen.	Door antwoord te geven op onderstaande vragen wordt de classificatie bepaald voor het betreffende aspect. Kies hiervoor een antwoord in de bijbehorende cel en voorzie het (indien gewenst) van een korte duidelijke motivatie. Deze motivatie maakt het mogelijk om de antwoorden op de vragen te controleren, op een later moment of door iemand anders. De uitkomst van de BIV-classificatie en de toelichting ervan is inzichtelijk in de volgende stap (3.). Neem bij het beantwoorden van de vragen het proces (het onderwijsproces of een specifiek ondersteunend proces) dat de ict-toepassing ondersteunt voor ogen. En, bedenk welke gegevens (bijvoorbeeld leerresultaten of leermateriaal) de ict-toepassing ondersteunt. N.B. De classificatie staat standaard op Hoog en kan verlaagd worden door het beantwoorden van alle vragen.	Door antwoord te geven op onderstaande vragen wordt de classificatie bepaald voor het betreffende aspect. Kies hiervoor een antwoord in de bijbehorende cel en voorzie het van een korte duidelijke motivatie. Deze motivatie maakt het mogelijk om de antwoorden op de vragen te controleren, op een later moment of door iemand anders. De uitkomst van de BIV-classificatie en de toelichting ervan is inzichtelijk in de volgende stap (3.). Neem bij het beantwoorden van de vragen het proces (het onderwijsproces of een specifiek ondersteunend proces) dat de ict-toepassing ondersteunt voor ogen. En, bedenk welke gegevens (bijvoorbeeld leerresultaten of leermateriaal) de ict-toepassing ondersteunt. N.B. De classificatie staat standaard op Hoog en kan verlaagd worden door het beantwoorden van alle vragen.	Voorleggen	We kunnen het door middel van deze afspraak niet verplichten, maar wel ontmoedigen. Daarom is de tekst aangepast en is '(indien gewenst)' verwijderd.
2024028	Stap 2.			Antwoorden zijn onnodig lang en niet consistent met de rest.	Op hoeveel gebruikers/organisaties heeft uitval impact? - Laag = bij uitval van de toepassing worden slechts enkele gebruikers/organisaties geraakt - Midden = bij uitval van de toepassing worden grote groepen gebruikers/organisaties geraakt - Hoog = bij uitval van de toepassing wordt een substantieel aandeel van de gebruikers/organisaties geraakt	Op hoeveel gebruikers heeft de uitval van de toepassing impact? - Laag: slechts een kleine groep gebruikers binnen de instelling wordt getroffen. - Midden: een groot aantal gebruikers binnen de instelling wordt getroffen. - Hoog: een substantieel deel van de gebruikers binnen de instelling wordt getroffen.	Voorleggen	Antwoorden anders geformuleerd. Daarnaast antwoorden ook relatief gemaakt, waardoor het beter aansluit op ieders situatie.

2024029	Stap 2.			Antwoorden kunnen duidelijker	Zijn er contractuele of wettelijke verplichtingen voor de beschikbaarheid? - Laag = nee of verplichtingen langer dan een dag - Midden = er zijn verpllichtingen: maximaal een dag onbeschikbaar - Hoog = er zijn verplichtingen: maximaal één uur onbeschikbaar	Zijn er contractuele of wettelijke verplichtingen (vanuit de instelling of leverancier) voor de beschikbaarheid? - Laag: nee, of verplichtingen staan een uitvaltijd van langer dan een dag toe - Midden: er zijn verplichtingen, met een maximale uitvaltijd van een dag - Hoog: er zijn verplichtingen, met een maximale uitvaltijd van één uur	Voorleggen	Antwoorden verduidelijkt; er is geen wijziging op de inhoud. Met name vanuit die deze verplichtingen gelden, na bespreking in de werksessie. Dit expliciet gemaakt door toevoeging: instelling of leverancier)
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 ict-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.	Voorleggen	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 ict-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.).	Voorleggen	Antwoorden Midden en Hoog aangepast. - Midden aangepast naar Onderwijs- en ontwikkelgegevens. - Hoog uitgebreid met Gevoelige persoonsgegevens met voorbeelden (o.b.v. de AP).
2024001	Stap 2.			de toelichting vaak te weinig concreet geformuleerd wat betreft het juist kunnen duiden van een 'midden' dan wel 'hoog' risico. Wat is bijvoorbeeld het verschil tussen:	'de gevolgen zijn beperkt' en 'materiële of immateriële schade dat leidt tot discriminatie of reputatieschade'		Vervalt	Geen concreet voorstel (meer) ontvangen.
2024005	Beschikbaarheid	E5, 6 en 7	Alle	Onduidelijk welke onderdelen minimaal meegenomen moeten worden	Naar aanleiding van deze analyse zijn de onderdelen van de toepassing (en de onderliggende infrastructuur) ingericht om overbelasting te voorkomen.	Naar aanleiding van deze analyse zijn de onderdelen van de toepassing (en de onderliggende infrastructuur, zoals servers, databases en applicatiecomponenten) ingericht om overbelasting te voorkomen.	Voorleggen	Ter verduidelijking toegevoegd: ", zoals servers, databases en applicatiecomponenten)"
2024006	Beschikbaarheid	G7	Hoog	Onduidelijk wat het verschil is tussen midden en hoog is	Na elke release wordt de beschikbaarheid en afname van performance direct getest door middel van een regressietest. Bij wijzigingen in het ontwerp of verwachte verandering in het gebruikersverkeer wordt er proactief een loadtest uitgevoerd met de verwachte load aan gebruikers/activiteiten. Deze test wordt uitgevoerd voordat de release wordt uitgerold en wordt niet - tijdens gebruikersuren - op productie uitgevoerd.	Na elke release wordt de beschikbaarheid en afname van performance direct getest door middel van een regressietest. Minimaal jaarlijks en bij wijzigingen in het ontwerp of verwachte verandering in het gebruikersverkeer wordt er proactief een loadtest uitgevoerd met de verwachte belasting aan gebruikers/activiteiten. Deze test wordt uitgevoerd voordat de release wordt uitgerold en wordt niet - tijdens gebruikersuren - op productie uitgevoerd.	Voorleggen	Er is geen verschil tussen midden en hoog; dat is bij meer maatregelen het geval. Wel is minimaal jaarlijks toegevoegd aan het begin van de 2e alinea.
2024008	Beschikbaarheid		Alle	Onduidelijk bij iedere classificatie hoe snel een dienst hersteld moet worden		Concreet maken binnen hoeveel dagen dienst hersteld moet zijn	Vervalt	Dit wordt reeds genoemd onder kenmerk van de classificatie
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 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 over de beschikbaarheid zijn opvraagbaar voor belanghebbenden.	Voorleggen	N.a.v. reden tot verzoek een aanvulling gedaan. Cijfers zijn opvraagbaar (zie laatste alinea)

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 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 over beschikbaarheid worden proactief na een afgesproken meetmoment medegedeeld (bijvoorbeeld via een portaal of servicegesprek) aan de belanghebbenden.	Voorleggen	N.a.v. reden tot verzoek een aanvulling gedaan. Cijfers worden proactief aangeboden (zie laatste alinea)
2024009	Integriteit	F6 en 7	Midden en 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 toepassing controleert invoer (handmatig of via geautomatiseerde koppeling) door bijvoorbeeld syntaxcontrole 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 - Gegevenskoppelingen worden automatisch gecontroleerd met behulp van syntaxcontrole en hashing.	Voorleggen	Er hoeft geen verschil te zijn. N.a.v. deze opmerking wel: regel toegevoegd voor hashing bij koppeling tussen systemen.
2024010	Integriteit	H5	Laag	Ontmoedigen = niet concreet auditbaar	Herleidbaar welke onderdelen/configuraties van de toepassing gewijzigd zijn: - Het is mogelijk om wijzigingen terug te draaien - Systeemaccounts met uitgebreide rechten zijn toegestaan - Toegang met root-accounts wordt ontmoedigd	Herleidbaar welke onderdelen/configuraties van de toepassing gewijzigd zijn: - Het is mogelijk om wijzigingen terug te draaien - Systeemaccounts met uitgebreide rechten zijn toegestaan - Toegang met root-accounts is gereguleerd, bijvoorbeeld met expliciete notificatie en logging	Voorleggen	Regel over gebruik root-account gelijkt getrokken met niveau midden.
2024012	Integriteit	J6	Midden	Onduidelijk met welke frequentie dit gedaan moet worden. Concreet maken periodiciteit logging controle	Gelogd wordt: inlogactiviteit technisch beheer, aanpassingen configuratie en toepassing Voor de kwaliteit van logging worden best practices gehanteerd (bijvoorbeeld OWASP Logging cheat sheet) De tijd van de applicatie is correct en consistent: wordt gesynchroniseerd met éénzelfde referentietijdbron als aanpalende systemen (binnen een netwerk of organisatie). Deze referentietijdbron is gesynchroniseerd met een publieke tijdsbron. Logging wordt periodiek (bijvoorbeeld maandelijks) gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera)	Gelogd wordt: inlogactiviteit technisch beheer, aanpassingen configuratie en toepassing Voor de kwaliteit van logging worden best practices gehanteerd (bijvoorbeeld OWASP Logging cheat sheet) De tijd van de applicatie is correct en consistent: wordt gesynchroniseerd met éénzelfde referentietijdbron als aanpalende systemen (binnen een netwerk of organisatie). Deze referentietijdbron is gesynchroniseerd met een publieke tijdsbron. Logging wordt periodiek (passend, maar ten minste maandelijks) gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera)	Voorleggen	Aangescherpt met "(passend, maar ten minste maandelijks)" i.p.v. "(bijvoorbeeld maandelijks.)" Hoe diepgaand je dit doet, is contextafhankelijk.
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 (gebruikersnaam en wachtwoord aangevuld met bijvoorbeeld een code op een mobiele telefoon, token of machine certificaat), bij toegang tot persoonsgegevens van (meerdere) derden. - 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 beheerder, maar ook docenten en leraren die toegang hebben tot anderemans persoonsgegevens. 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.

2024015	Vertrouwelijkheid	J7	Hoog	Vereiste is onduidelijk. Logging en de monitoring moet voldoen aan de vereisten van ISO, NK IBP FO. Tevens dient de onderwijinstelling zelf te kunnen monitoren. Thans wordt met Topicus een heel logging/monitoring dashboard ontwikkeld voor de applicatie van Somtoday. Goed om dit eens met elkaar door te spreken waaraan dit moet voldoen.	Toegang tot de applicatie (zowel gelukt als mislukt) en lezen van (persoons)gegevens wordt gelogd. Logging is enkel toegankelijk voor bevoegde personen (op basis van autorisatie) en toegang ertoe wordt apart gelogd. Beide logging wordt regelmatig gecontroleerd op uitzonderingen op toegang en uitzonderlijke patronen in gebruik. Bijvoorbeeld door automatische loganalysetooling.	Toegang tot de applicatie (zowel gelukt als mislukt) en lezen van (persoons)gegevens wordt gelogd. Logging is enkel toegankelijk voor bevoegde personen (op basis van autorisatie) en toegang ertoe wordt apart gelogd. Beide logging wordt regelmatig gecontroleerd op uitzonderingen op toegang en uitzonderlijke patronen in gebruik. Deze logging is toegankelijk of z.s.m. opvraagbaar door de afnemer van de applicatie.	Voorleggen	Opvraagbaar toegevoegd, zodat scholen dit kunnen opvragen als er situaties naar vragen (datalek of misbruik oid).
2024016	Vertrouwelijkheid	D6	Midden	Onduidelijk wat 'overschrijven' toevoegd	Er wordt invulling gegeven aan wettelijke bewaartermijnen voor persoonsgegevens, logging, leerlingdossiers, et cetera. De applicatie moet het mogelijk maken dat persoonsgegevens verwijderd moeten kunnen worden, bijvoorbeeld op verzoek van de betrokkene of wanneer de bewaartermijn verstreken is. Op media/apparatuur die niet meer worden gebruikt of voor andere doeleinden worden hergebruikt wordt data gewist én overschreven.	Er wordt invulling gegeven aan wettelijke bewaartermijnen voor persoonsgegevens, logging, leerlingdossiers, et cetera. De applicatie moet het mogelijk maken dat persoonsgegevens verwijderd moeten kunnen worden, bijvoorbeeld op verzoek van de betrokkene of wanneer de bewaartermijn verstreken is. Op media/apparatuur die niet meer worden gebruikt of voor andere doeleinden worden hergebruikt wordt data onherstelbaar vernietigd (bijvoorbeeld degaussing, sanitization, purging, zeroization of vernietiging van de (verwijderbare) media).	Voorleggen	Gelijkgetrokken met niveau Hoog wat betreft data vernietiging.
2024018	Vertrouwelijkheid	H6 en 7	Midden en Hoog	Onduidelijk welke extra maatregelen genomen moeten worden bij Hoog ten opzichte van Midden	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) mag niet worden gebruikt in OTA. Gebruik in OTA dummy data Toegang tot OTAP wordt beheerd en ieder kwartaal 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.	Vervalt	Dit wordt reeds opgepakt onder 2024027
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	Voorleggen	Naast bijzondere worden ook gevoelige persoonsgegevens genoemd, zoals nu ook in Stap 2. wordt benoemd.
2024022							Vervalt	RFC regels is leeg.