Inleiding

Dit is het toetsingskader behorende bij het Certificeringsschema Informatiebeveiliging en Privacy ROSA. De volgende documenten beschrijven hoe je deze moet toepassen:
- Certificeringsschema algemene beschrijving
- Certificeringsschema proces (beschrijf de analyse en toepassing toetsingskader)
- Certificeringsschema toezicht (beschrijft de vastlegging van resultaten)

Doel en gebruik

Dit toetsingskader presenteert de maatregelen voor een ict-toepassing op basis van de BIV-classificatie van de ict-toepassing. Begin hiervoor bij tabblad 'Stap 1.' en vul daar de stamgegevens in. Vervolgens kan in de volgende stap (2.) de classificatie bepaald worden door beantwoording van alle vragen. De uitkomst hiervan - de BIV-classificatie - is zichtbaar in stap 3. Deze wordt gebruikt als input in stap 4. waarin de benodigde maatregelen worden aangewezen. In deze stap (4.) kan de status van de maatregelen aangegeven worden. In het laatste tabblad 'Rapportage' staat informatie samengevat, zoals de status van implementatie incl. de toetsing daarvan.

Daarbij geldt dat:
- De maatregelen beperken zich nadrukkelijk tot het technisch domein.
- De maatregelen moeten op basis van het comply-or-explain principe worden beoordeeld.
- Maatregelen op het gebied van organisatie en proces zijn momenteel buiten scope van het certificeringsschema. Het is echter wel mogelijk dat maatregelen op het gebied van organisatie en proces maatregelen op technisch niveau overbodig maken.

Versie historie

Datum	Versie	Auteur	Commentaar
6/27/2017	1.0	Werkgroep IBP	Verwerken laatste opmerkingen
2/23/2022	2.1	Jordy van den Elshout	Alle RFC's 2021 doorgevoerd, versie ter review aan de
3/15/2022	2.2	Werkgroep IBP	Verwerken laatste opmerkingen

3/17/2022	2.3	Jordy van den Elshout	Functionele uitbreiding: 1) Overzicht met maatregelen op basis van BIV en 2) Automatisch rapport voor bijlage 2 (Privacyconvenant)
4/6/2022	2.4	Jordy van den Elshout	Wensen van de werkgroep IBP doorgevoerd, zoals toevoegen classificatievragen
4/12/2022	3.0	Jordy van den Elshout	Versie ter goedkeuring

Vul hier de stamgegevens in. Op basis hiervan wordt de rapportage op het laatste tabblad ingevuld.

Stamgegevens van het product of de dienst

Productnaam	:	SchoolWebsite, SchoolApp, SchoolSchermen en Kidsplace
Bedrijfsnaam	:	SchoolsUnited b.v.
URL product	:	schoolsunited.eu

Classificatie (Stap 2) wordt uitgevoerd door

Naam	:	R. Verbeek i.s.m. PrivacyOpSchool
Functie	:	directeur , voor vragen: richardverbeek@schoolsunited.eu

Maatregelen (Stap 4) worden getoetst door

Naam	:	Tim Smallenberg van Smallhold b.v
Functie	:	directeur
Naam organisatie	:	Smallhold b.v.
Toetsvorm	:	Self-assessment
Uitgevoerd op	:	2/14/2023

Doel en gebruik

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.

Beschikbaarheid

Niveau Midden

Selecteer het antwoord en motiveer deze

Vragen	Antwoord	Motivatie
Wanneer **moet** de dienst beschikbaar zijn voor de gebruikers? - Laag = regulier (bijvoorbeeld alleen kantooruren) - Midden = ruim (bijvoorbeeld 07:00 - 23:00 en/of ook in het weekend) - Hoog = altijd (bijvoorbeeld 24x7)	Midden	de software wordt voor 99% gebruikt tussen 7.00 - 23.00 , daartussen is er nauwelijks internettraffic.
Wat is de langste periode dat de ict-toepassing niet beschikbaar mag zijn? - Laag = maximaal enkele dagen - Midden = maximaal een aantal uur - Hoog = maximaal een aantal minuten	Midden	Bij een grote storing (bijvoorbeeld uitval of een significante bug) is het acceptabel deze binnen 12 uur na het ontstaan
Welke impact heeft uitval (de data, informatie of de ict-toepassing zijn niet beschikbaar)? - Laag = geen - Midden = het proces wordt belemmerd maar kan wel doorgaan - Hoog = het proces kan in zijn geheel niet doorgaan	Midden	De school kan doorfunctioneren. Gebruikers van de app ondervinden hinder in de communicatie tussen ouders en de school. De website werkt niet

Integriteit

Niveau Midden

Selecteer het antwoord en motiveer deze

Vragen	Antwoord	Motivatie
Kan er misbruik plaatsvinden - bijvoorbeeld fraude met leerresultaten of financiële fraude - door fouten in de gegevens of ongeautoriseerde wijzigingen? - Laag = nee, de gegevens lenen zich niet voor misbruik - Midden = beperkt, gegevens worden ook elders gecontroleerd - Hoog = ja, de ict-toepassing is de enige toepassing met deze gegevens	Midden	Er wordt beperkt informatie opgeslagen van ouders; e-mail, naam, eventueel adres en tel. nnr. en heel beperkt van de kinderen (in welke groep ze zitten, verjaardag)
Kunnen er personen negatieve gevolgen ondervinden als gevolg van het niet correct zijn van gegevens? - Laag = niet - Midden = eventuele fouten zijn nog te corrigeren - Hoog = fouten veroorzaken ernstige of langdurige negatieve gevolgen	Midden	Tijdelijk zeer beperkte hinder, bijvoorbeeld omdat een kind niet aan de juiste groep gekoppeld is. Maar ouders kunnen zelf hun
Wat is het effect op het onderwijs- of ondersteunend proces als fouten of ongeautoriseerde veranderingen in de gegevens zitten? - Laag = geen - Midden = het proces wordt belemmerd maar kan wel doorgaan - Hoog = het proces kan in zijn geheel niet doorgaan	Midden	Het proces van de app en de website kan tijdelijk verstoord worden, maar het kernproces van de school wordt niet verstoord.

Vertrouwelijkheid

Niveau Hoog

Selecteer het antwoord en motiveer deze

Vragen	Antwoord	Motivatie
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.	Hoog	De chat module en de absentiemodule bevat potentieel bijzondere persoongegevens, echter de chatgegevens en de absentiegegevens worden eens per jaar op 1/8 gewist.
Leidt openbaarmaking van de gegevens (bv. van examenvragen) of datalek van persoonsgegevens tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies wat opgevangen kan worden door tijdige communicatie - Hoog = langdurig imagoverlies	Midden	De aard van de gegevens zou in theorie tot beperkt imagoverlies kunnen leiden maar is
Kunnen er personen schade ondervinden als gevolg van het uitlekken van de gegevens? - Laag = niet - Midden = ja, maar de gevolgen zijn beperkt - Hoog = ja, fysieke, materiële of immateriële schade. Zoals: discriminatie, (identiteits-)fraude, financiële schade en reputatieschade.	Midden	In theorie zou dat kunnen maar lijkt in de praktijk vergezocht. Er worden beperkt

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	Midden	De basis van de school werkt gewoon door, er is op de dag van de storing enige hinder omdat communicatie via website of app of een deel daarvan niet mogelijk is.
Zijn er contractuele of wettelijke verplichtingen voor de beschikbaarheid? - Laag = nee of verplichtingen langer dan een dag - Midden = er zijn verplichtingen: maximaal een dag onbeschikbaar - Hoog = er zijn verplichtingen: maximaal één uur onbeschikbaar	Midden	SchoolsUnited heeft de inspanningsverplichting omn er alles aan te doen een grote storing binnen 24 uur te verhelpen.

In hoeverre hebben fouten of ongeautoriseerde veranderingen in gegevens invloed op andere toepassingen? - Laag = geen; alleen in de toepassing - Midden = aanzienlijk; ook in andere toepassing (en), door (hergebruik gegevens. - Hoog = groot effect door bijvoorbeeld automatische beslissingen, veel koppelingen en veel transacties	Laag	Er is geen koppeling met andere systemen.
Leiden fouten of ongeautoriseerde veranderingen tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies - Hoog = langdurig imagoverlies	Midden	op de website en in de app zouden kortstondig negatieve en verkeerde informatie kunnen komen te staan, maar de website
Zijn er contractuele of wettelijke verplichtingen voor de integriteit van gegevens? - Laag = nee - Midden = ja, deze eisen stelselmatige controle (denk aan examenresultaten) - Hoog = ja, deze eisen stelselmatige controle en bewijs van werking (denk aan gegevens ten behoeve van bekostiging)	Laag	SchoolsUnited zet zich als leverancier maximaal in voor de integriteit van de gegevens., zoals een goed leverancier van dit soort producten betaamt. In die zin
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)	Laag	nee, niet van toepassing.
Hoe actueel moeten de gegevens na herstel zijn, totdat dit tot problemen leidt? - Laag = Gegevens mogen enkele dagen oud zijn. - Midden = Gegevens mogen niet ouder dan 24 uur zijn - Hoog = Gegevens mogen niet ouder dan 4 uur	Laag	op zich mogen de gegevens enkele dagen oud zijn zonder dat dit gelijk tot signifiance

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	Laag	niet van toepassing
Leidt het uitlekken van de gegevens tot economische schade? - Laag = nee - Midden = beperkte economische schade - Hoog = aanzienlijke economische schade	Laag	niet van toepassing

* Onder profilering verstaat de AVG "elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen" [bron: artikel 4 van de AVG]

Doel en gebruik

Neem kennis van onderstaande BIV-classificatie. Deze wordt automatisch ingevuld op basis van de antwoorden die in stap 2. zijn gegeven. De classificatie staat standaard op Hoog en kan verlaagd worden door het beantwoorden van alle vragen in stap 2. Indien de BIV reeds bepaald is, dan kan deze in onderstaande overzicht ook handmatig aangepast worden.

Let op! Pas de BIV-classificatie niet meer aan, nadat de volgende stap is ingevuld. Dan corresponderen de maatregelen niet meer met de ingevulde status.

Let op! Onderstaande BIV is handmatig ingevuld en wordt niet meer automatisch bijgewerkt op basis van de antwoorden in stap 2.

BIV-Classificatie

Beschikbaarheid	Intergriteit	Vertrouwelijkheid
Midden	**Midden**	Midden
Toelichting	**Toelichting**	**Toelichting**
Beschikbaarheid is belangrijk. Algeheel verlies of niet beschikbaar zijn van deze applicatie gedurende een dag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	Integriteit is belangrijk. Blijvende juistheid van informatie is belangrijk, maar sommige toleranties zijn toelaatbaar. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet volledig, correct of actueel is, leidt dit tot substantiële schade.	Informatie is vertrouwelijk. De organisatie, instelling of betrokkene kan substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know basis). Hieronder vallen onder andere persoonsgegevens.
Kernmerken	**Kernmerken**	**Kernmerken**
Herstel van de dienst mag niet langer dan 24 uur bedragen.	Bedrijfsproces tolereert een zeer beperkt aantal fouten. Gegevens zijn volledig, juist en actueel; Maximaal toegestaan dataverlies na herstel: 24 uur.	Alleen toegankelijk voor direct betrokkenen binnen de organisatie op basis van functie of rol.

Doel en gebruik

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).

Beschikbaarheid	Niveau Midden
Maatregel	Status en toelichting
Ontwerp	Voldaan
Tijdens het ontwerp is gekeken naar de afhankelijkheden van aanpalende systemen (zowel intern als extern, zoals van leveranciers of ketenpartners) en impact van eventuele uitval. Naar aanleiding van deze analyse zijn de onderdelen van de toepassing ingericht om kennisgeving van uitval te geven. Infrastructuur bestaat uit: - active-passive applicatieonderdelen - (passieve) backup netwerkverbinding - redundante aansluiting voeding	*De servers zijn o.a. opgezet volgens een RAID-systeem, waarbij twee harddisks dezelfde inhoud hebben. Als één harddisk om wat voor reden dan ook faalt kan de ander het dus probleemloos overnemen. Verder wordt er iedere dag ('s nachts) een volledige back-up van alle gebruikersdata gemaakt. Van die back-ups bewaren we er steeds dertig op rij. De back-ups staan bovendien op een fysiek andere locatie opgeslagen.*
Capaciteit beheer	Voldaan
De hoeveelheid gebruikersverkeer is tijdens het ontwerp van de toepassing bepaald en wordt proactief bijgesteld op basis van een trendanalyse of verwachte aantallen. Naar aanleiding van deze analyse zijn de onderdelen van de toepassing (en de onderliggende infrastructuur) ingericht om overbelasting te voorkomen. Het gebruikersverkeer en het effect daarvan wordt gemonitord, zoals het disk, geheugen- en of processorgebruik. Op basis van een voorafgestelde norm vindt actieve signalering plaats, zodat extra resources toegewezen kunnen worden.	*Er wordt een uitgebreide set van tools gebruikt om dit soort parameters te testen en dit wordt real time gemonitord en waar nodig vindt signalering naar de beheerder plaats.*
Onderhoud	Voldaan

Integriteit van de gegevens

Integriteit	Niveau Midden
Maatregel	Status en toelichting
Herleidbaarheid (gebruikers)	Alternatieve maatregel
Herleidbaar wanneer, welke gegevens gewijzigd zijn: - Gebruikers hebben standaard (by default) niet meer rechten dan nodig: least privilege - Het is mogelijk om wijzigingen terug te draaien - Naamloze gebruikersaccounts met uitgebreide rechten zijn toegestaan maar (indirect) herleidbaar naar personen - Herleidbaar wanneer de gegevens gewijzigd zijn - Gebruikers mogen beheerdersrechten hebben - Wijziging van gegevens is inzichtelijk, zodat een analyse hierop mogelijk is.	*De aard van de software, het bijhouden van de website en van een app, is relatief simpel en bijhouden van op ieder moment wie wat gewijzigd heeft is bij het ontwerp van de software niet over geïmplementeerd en is achteraf niet realistisch om te implementeren. Wel is er logging wie wanneer is ingelogd geweest en ook is de back-up procedure heel goed ingericht, zodat bij wijzigingen back-ups tot 30 dagen oud teruggezet kunnen worden. Op serverniveau worden cruciale wijzigen constant gemonitord en wijzigingen opgeslagen, dus op bepaalde niveaus wordt er wel voldaan maar niet op alle niveaus.*
Backup	Voldaan
Backup is verplicht, minimaal 1 keer per dag, bijvoorbeeld door snapshots. Integriteit van de back-up wordt periodiek (min. 1x per kwartaal) gecontroleerd. Backup wordt beschermd door functiescheiding en fysieke scheiding: opslag op een andere locatie.	*Iedere nacht wordt er een back-up gemaakt die op een andere locatie wordt opgeslagen. Back-ups worden 30 dagen bewaard*
Application controls	Voldaan

Vertrouwelijkheid	Niveau Midden
Maatregel	Status en toelichting
Levenscyclus gegevens	Voldaan
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.	*Gebruikers kunnen grotendeels hun eigen data verwijderden en chatgegevens / absentiegegevens worden eens per jaar verwijderd. De school is daarnaast ook zelf verantwoordelijk voor het opschonen van data en/of dit verplaatsen naar een archief. In jaarovergang.pdf vinden gebruikers een checklist met waar ze zelf op dienen te letten, deze is te downloaden vanaf onze website.*
Logische toegang	Voldaan
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.	*Er is voor superusers een set veiligheidsmaatregelen genomen die we hier omwille van de veiligheid niet nader specificeren.*
Fysieke toegang	Voldaan

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.	*Het is een dagelijks proces van het in de gaten houden of de meest relevante updates, vernieuwingen, patches etc. zijn uitgevoerd of dat hier actie voor nodig is, dit wordt heel adequaat uitgevoerd om ervoor te zorgen dat de servers en de software maximaal veilig zijn.*
Testen	Voldaan
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.	*Er wordt bij een nieuwe release uiterst zorgvuldig gekeken wat het effect daarvan is en er wordt bij belangrijke wijzigingen in de nacht, in het weekend of in een schoolvakantie aanpassingen uitgevoerd.*
Monitoring	Voldaan
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.	*Cruciale processen wordt real-time gemonitord door de software op de server en indien nodig vindt er een alert plaats dmv een e-mail naar de beheerder te sturen. Er wordt onmiddellijk actie ondernomen door het softwarematig te herstellen of zonodig af te reizen naar het datacentrum om hardware te vervangen.*
Herstel	Voldaan

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	*Er wordt zeer uitgebreid gecontroleerd op de syntax om fouten af te vangen. Er vindt geen uitvoer naar andere systemen plaats en er is monitoring op hackers die trachten onderdelen van de software te misbruiken zoals het proberen te injecteren van foute code of formulieren te misbruiken.*
Onweerlegbaarheid	Alternatieve maatregel
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)	*Er is sprake van logging van gebruikers maar niet in de zin van dat alle wijzigingen worden vastgelegd.*
Herleidbaarheid (technisch beheer)	Voldaan
Herleidbaar wanneer, welke onderdelen/configuraties van de toepassing gewijzigd zijn: - Het is mogelijk om wijzigingen terug te draaien - Naamloze systeemaccounts met uitgebreide rechten zijn toegestaan en (indirect) herleidbaar naar personen - Herleidbaar wanneer de toepassing gewijzigd is - Toegang tot de onderliggende systemen van de toepassing is rolgebaseerd toegewezen - Toegang met root-accounts is gereguleerd, bijvoorbeeld met expliciete notificatie en logging	*Er zijn heldere procedures voor het uitrollen van nieuwe software en het terugvallen op een roll-back.*
Controle integriteit	Voldaan

Fysieke toegang tot de apparatuur waar de toepassingen en de data verwerkt wordt, is beschermd met minimaal: - Eén factor authenticatie - Logging en monitoring van toegang, bijvoorbeeld cameratoezicht voor de herleidbaarheid. Bezoekers enkel onder begeleiding.	*Het datacenter is streng beveiligd en voldoet aan de hoogste beveiligingscertificaten. Zie https://www.dataplace.com/over-ons/onze-datacenters-nederland/dataplace-nedzone voor details.*
Netwerk toegang	Voldaan
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	*Zulke maatregelen zijn er, zoals inderdaad het dichtzetten van poorten, geoblocking en het beperken van super-user-toegang tot een beperkte groep medewerkers aan de hand van specifieke IP-adressen en volgens strikte authenticatie.*
Scheiding omgevingen	Voldaan
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.	*Er is een ontwikkelomgeving, testomgevingen die eerst geaccepteerd moeten worden alvorens dit naar de productieomgeving gaat (test en acceptatie zit in één omgeving gezien de bescheiden schaal van de software).*
Transport en fysieke opslag	Voldaan

Er is een 'Warm Standby' aanwezig, dat wil zeggen: nieuwe fysieke of virtuele infrastructuur kan gelijk in gebruik genomen worden maar vergt nog wel enkele handelingen zoals het overzetten van gegevens. Herstel door opnieuw opstarten/inspoelen van de toepassing (verlies van enkele sessies en transacties toegestaan). Recovery test: 1x per jaar. Herstel van de dienst mag niet langer dan 24 uur bedragen.	*Er kan vanaf de back-up server real-time een backup teruggezet worden en er zijn van veel componenten spare parts aanwezig. Omdat sommige gebruikers soms per ongeluk delen van de software wissen vindt gedurende het jaar regelmatig een recovery plaats zodat sowieso altijd binnen de tijdspanne van 1 jaar gebruik gemaakt wordt van de back-up server.*

Integriteit van de toepassing	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	*Het zit in het DNA van de organisatie om kwetsbaarheden te monitoren en daar waar nodig aan te passen om zo maximaal mogelijk veilig te zijn tegen hackers. Dit is een constant proces van monitoring door onszelf en Smallhold B.V.*
	Onweerlegbaarheid (Toepassing)	Voldaan
	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)	*Er worden door de server een grote hoeveelheid kernprocessen gelogd, en die logging wordt regelmatig, zowel automatisch (met een melding als er afwijkingen gedecteerd worden) als manueel gecontroleerd op problemen en afwijkingen. Er wordt met de atoomklok die gangbaar is op internet dagelijks gesynchroniseerd.*

Encryptie van transport (zowel voor intern als extern verkeer) is conform de meest recente versie van Uniforme Beveiligingsvoorschriften (UBV) TLS van Edustandaard. Encryptie van opslag, moet minimaal op (virtuele)disk-levelniveau. Hiervoor wordt gebruik gemaakt van richtlijnen/best practices/standaarden, zoals van NCSC, ENISA, NIST.	*Er vindt vanuit onze applicatie geen transport naar andere educatieve applicaties plaats, dus dit deel is niet van toepassing. Wel vindt uiteraard encryptie van wachtwoorden en data plaats op de server en moet een school verplicht met een SSL-certificaat werken om met de software te mogen werken.*
Logging	Niet voldaan
Toegang tot de applicatie (zowel gelukt als mislukt) en lezen van (persoons)gegevens wordt gelogd. Logging is enkel toegankelijk voor bevoegde personen en toegang ertoe wordt apart gelogd.	*Tegang tot de applicatie wordt gelogd, maar welke gegevens door wie worden gelezen wordt niet gelogd.*
Omgaan met kwetsbaarheden	Alternatieve maatregel

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.	*Er worden op basis van de wet van het voortschrijdend inzicht regelmatig nieuwe procedures of software geïmplementeerd om kwetsbaarheden op te lossen dan wel te voorkomen. Veel heeft te maken met hackers/spammers die constant nieuwe dingen uitproberen om via de servers spam te versturen. De servers zijn zo ingericht dat alleen het hoogst noodzakelijk nodig is voor de software die erop draait, welke enkel de dedicated software is die SchoolsUnited b.v. zelf laat ontwikkelen, waardoor kwetsbaarheden sowieso al veel meer beperkt worden.*

Doel en gebruik

Onderstaande rapport wordt automatisch opgemaakt op basis van de gegevens uit de voorgaande tabbladen (advies is omgewenste wijzigingen daar aan te brengen). Onderstaande tabel kan één op één overgenomen als rapportage in bijlage 2 van de model verwerkersovereenkomst van Convenant digitale onderwijsmiddelen en privacy. Zie www.privacyconvenant.nl voor meer informatie

Toetsvorm	self assesment		
Uitvoerder toets	richard verbeek		
Inlogpagina	schoolsunited.eu		
BIV-classificatie	Beschikbaarheid=Midden || Integriteit=Midden || Vertrouwelijkheid=Midden		
Categorie	**Maatregelen**	**Compliance**	**Uitleg**
		[Voldaan/niet voldaan/ alternatieve maatregel]	[Bij niet voldaan aangeven hoe/wanneer dit wordt gecorrigeerd. Bij alternatieve maatregel deze beschrijven]
Beschikbaarheid	Ontwerp	Voldaan	De servers zijn o.a. opgezet volgens een RAID-systeem, waarbij twee harddisks dezelfde inhoud hebben. Als
	Capaciteit beheer	Voldaan	Er wordt een uitgebreide set van tools gebruikt om dit soort parameters te testen en dit wordt real-time
	Onderhoud	Voldaan	Het is een dagelijks proces van het in de gaten houden of de meest relevante updates, vernieuwingen
	Testen	Voldaan	Er wordt bij een nieuwe release uiterst zorgvuldig gekeken wat het effect daarvan is en er wordt bij belangrijke
	Monitoring	Voldaan	Cruciale processen wordt real-time gemonitord door de software op de server en indien nodig vindt er een
	Herstel	Voldaan	Er kan vanaf de back-up server real-time een backup teruggezet worden en er zijn van veel componenten spare
Integriteit	Herleidbaarheid (gebruikers)	Alternatieve maatregel	De aard van de software,het bijhouden van de website en van een app, is relatief simpel en bijhouden van op
	Backup	Voldaan	Iedere nacht wordt er een back-up gemaakt die op een andere locatie wordt opgeslagen. Back-ups worden
	Application controls	Voldaan	Er wordt zeer uitgebreid gecontroleerd op de syntax om fouten af te vangen. Er vindt geen uitvoer naar andere
	Onweerlegbaarheid	Alternatieve maatregel	Er is sprake van logging van gebruikers maar niet in de zin van dat alle wijzigingen worden vastgelegd

	Herleidbaarheid (technisch beheer)	Voldaan	Er zijn heldere procedures voor het uitrollen van nieuwe software en het terugvallen op een roll-back
	Controle integriteit	Voldaan	Het zit in het DNA van de organisatie om kwetsbaarheden te monitoren en daar waar nodig aan te passen om ze
	Onweerlegbaarheid (toepassing)	Voldaan	Er worden door de server een grote hoeveelheid kernprocessen gelogd, en die logging wordt regelmatig, zowel
Vertrouwelijkheid	Levenscyclus gegevens	Voldaan	Gebruikers kunnen grotendeels hun eigen data verwijderden en chatgegevens / absentiegegevens
	Logische toegang	Voldaan	Er is voor superusers een set veiligheidsmaatregelen genomen die we hier omwille van de veiligheid niet
	Fysieke toegang	Voldaan	Het datacenter is streng beveiligd en voldoet aan de hoogste beveiligingscertificaten. Zie https:
	Netwerk toegang	Voldaan	Zulke maatregelen zijn er, zoals inderdaad het dichtzetten van poorten, geoblocking en het beperken van
	Scheiding omgevingen	Voldaan	Er is een ontwikkelomgeving, testomgevingen die eerst geaccepteerd moeten worden alvorens
	Transport en fysieke opslag	Voldaan	Er vindt vanuit onze applicatie geen transport naar andere educatieve applicaties plaats, dus dit deel is niet
	Logging	Niet voldaan	Tegang tot de applicatie wordt gelogd, maar welke gegevens door wie worden gelezen wordt niet gelogd
	Omgaan met kwetsbaarheden	Alternatieve maatregel	Er worden op basis van de wet van het voortschrijdend inzicht regelmatig nieuwe procedures of software

Toelichting

Dit is het einde. Ter naslag zijn ook alle maatregelen per informatiebeveiligingsaspect beschikbaar. Zie hiervoor de blauw opvolgende tabbladen. Deze tabbladen worden gebruikt voor het presenteren de maatregelen in stap 4.

			Maatregelen					
			Ontwerp	**Capaciteit beheer**	**Onderhoud**	**Testen**	**Monitoring**	**Herstel**
Beschikbaarheid	**Omschrijving**	**Kenmerken**						
Laag	Beschikbaarheid is minder belangrijk. Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende meer dan een dag brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	Herstel van de dienst mag langer dan 24 uur bedragen.	Tijdens het ontwerp is gekeken naar de afhankelijkheden van aanpalende systemen (zowel intern als extern, zoals van leveranciers of ketenpartners) en impact van eventuele uitval. Infrastructuur mag bestaan uit: - enkelvoudige applicatieonderdelen - enkelvoudige verbindingen - enkelvoudige aansluiting voeding	De hoeveelheid gebruikersverkeer is tijdens het ontwerp van de toepassing bepaald. Naar aanleiding van deze analyse zijn de onderdelen van de toepassing (en de onderliggende infrastructuur) ingericht om overbelasting te voorkomen.	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.	Onbeschikbaarheid wordt ad-hoc behandeld bv. op basis van een melding van een gebruiker. Beschikbaarheidsincidenten worden geregistreerd.	Terwijl de toepassing wordt gebruikt, wordt de beschikbaarheid van de toepassing en aanpalende toepassingen gemonitord.	Er is een 'Cold Standby' aanwezig, dat wil zeggen: nieuwe fysieke of virtuele infrastructuur is beschikbaar maar nog niet ingericht. Manueel herstel van de toepassing en gegevens. Recovery test: 1x per 2 jaar. De dienst is in enkele dagen te herstellen.
Midden	Beschikbaarheid is belangrijk. Algeheel verlies of niet beschikbaar zijn van deze applicatie gedurende een dag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	Herstel van de dienst mag niet langer dan 24 uur bedragen.	Tijdens het ontwerp is gekeken naar de afhankelijkheden van aanpalende systemen (zowel intern als extern, zoals van leveranciers of ketenpartners) en impact van eventuele uitval. Naar aanleiding van deze analyse zijn de onderdelen van de toepassing ingericht om kennisgeving van uitval te geven. Infrastructuur bestaat uit: - active-passive applicatieonderdelen - (passieve) backup netwerkverbinding - redundante aansluiting voeding	De hoeveelheid gebruikersverkeer is tijdens het ontwerp van de toepassing bepaald en wordt proactief bijgesteld op basis van een trendanalyse of verwachte aantallen. Naar aanleiding van deze analyse zijn de onderdelen van de toepassing (en de onderliggende infrastructuur) ingericht om overbelasting te voorkomen. Het gebruikersverkeer en het effect daarvan wordt gemonitord, zoals het disk, geheugen- en of processorgebruik. Op basis van een voorafgestelde norm vindt actieve signalering plaats, zodat extra resources toegewezen kunnen worden.	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.	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.	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.	Er is een 'Warm Standby' aanwezig, dat wil zeggen: nieuwe fysieke of virtuele infrastructuur kan gelijk in gebruik genomen worden maar vergt nog wel enkele handelingen zoals het overzetten van gegevens. Herstel door opnieuw opstarten/inspoelen van de toepassing (verlies van enkele sessies en transacties toegestaan). Recovery test: 1x per jaar. Herstel van de dienst mag niet langer dan 24 uur bedragen.

Hoog	Beschikbaarheid is noodzakelijk. Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	Herstel van de dienst mag niet langer dan 8 uur bedragen.	Tijdens het ontwerp is gekeken naar de afhankelijkheden van aanpalende systemen (zowel intern als extern, zoals van leveranciers of ketenpartners) en impact van eventuele uitval. Naar aanleiding van deze analyse zijn de onderdelen van de toepassing ingericht om kennisgeving van uitval te geven. Er wordt regelmatig opnieuw geanalyseerd wat de afhankelijkheden met andere toepassingen zijn. Bijvoorbeeld bij grote wijzigingen, aanpassingen of verandering in gebruikersverkeer. Infrastructuur bestaat uit: - active-active applicatieonderdelen - actieve backup netwerkverbinding - UPS/NoBreak	De hoeveelheid gebruikersverkeer is tijdens het ontwerp van de toepassing bepaald en wordt proactief bijgesteld op basis van een trendanalyse of verwachte aantallen. Naar aanleiding van deze analyse zijn de onderdelen van de toepassing (en de onderliggende infrastructuur) ingericht om overbelasting te voorkomen. Het gebruikersverkeer en het effect daarvan wordt gemonitord, zoals het disk-, geheugen- en of processorgebruik. Op basis van een voorafgestelde norm vindt actieve signalering plaats, zodat extra resources toegewezen kunnen worden. Overbelasting (ook door mogelijke DDoS) wordt gereguleerd door middel van firewall, load balancers, traffic shaper of een soortgelijk oplossingen. Resources worden automatisch toegewezen.	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.	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.	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.	Er is een 'Hot Standby' aanwezig, dat wil zeggen: de toepassing draait reeds op fysieke of virtuele reserve-infrastructuur waar direct naar overgeschakeld kan worden. Automatische online failover (verlies van sessies en transacties wordt voorkomen). Recovery test: 2x per jaar. Herstel van de dienst mag niet langer dan 8 uur bedragen.

			Maatregelen						
			Integriteit van de gegevens				***Integriteit van de toepassing***		
			Herleidbaarheid (gebruikers)	**Backup**	**Application controls**	**Onweerlegbaarheid**	**Herleidbaarheid (technisch beheer)**	**Controle integriteit**	**Onweerlegbaarheid (Toepassing)**
Integriteit	**Omschrijving**	**Kenmerken**							
Laag	Integriteit is minder belangrijk. Blijvende juistheid van informatie is gewenst, maar hoeft niet gegarandeerd te zijn. Indien informatie niet volledig, correct of actueel is, leidt dit tot beperkte schade.	Bedrijfsproces tolereert enkele fouten Gegevens zijn volledig. Maximaal toegestaan dataverlies na herstel: enkele dagen.	Herleidbaar welke gegevens gewijzigd zijn: - Het is mogelijk om wijzigingen terug te draaien - Naamloze gebruikersaccounts met uitgebreide rechten zijn toegestaan - Gebruikers mogen beheerdersrechten hebben	Backup is verplicht, minimaal wekelijks, bijvoorbeeld door een script. Integriteit van de back-up wordt ad-hoc, maar minimaal 1 keer jaar, gecontroleerd.	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.	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)	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	Ad hoc controle integriteit toepassing: - De status van doorgevoerde patches en updates van firmware en software worden ad-hoc gecontroleerd - Integriteit van de configuratie en software wordt handmatig gecontroleerd Maatregelen tegen malware zijn toegepast Secure software development/secure coding guidelines worden toegepast	Gelogd wordt: inlogactiviteit technisch beheer Voor de kwaliteit van logging worden best practices overwogen (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.
Midden	Integriteit is belangrijk. Blijvende juistheid van informatie is belangrijk, maar sommige toleranties zijn toelaatbaar. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet volledig, correct of actueel is, leidt dit tot substantiële schade.	Bedrijfsproces tolereert een zeer beperkt aantal fouten. Gegevens zijn volledig, juist en actueel; Maximaal toegestaan dataverlies na herstel: 24 uur.	Herleidbaar wanneer, welke gegevens gewijzigd zijn: - Gebruikers hebben standaard (by default) niet meer rechten dan nodig: least privilege - Het is mogelijk om wijzigingen terug te draaien - Naamloze gebruikersaccounts met uitgebreide rechten zijn toegestaan maar (indirect) herleidbaar naar personen - Herleidbaar wanneer de gegevens gewijzigd zijn - Gebruikers mogen beheerdersrechten hebben - Wijziging van gegevens is inzichtelijk, zodat een analyse hierop mogelijk is.	Backup is verplicht, minimaal 1 keer per dag, bijvoorbeeld door snapshots. Integriteit van de back-up wordt periodiek (min. 1x per kwartaal) gecontroleerd. Backup wordt beschermd door functiescheiding en fysieke scheiding: opslag op een andere locatie.	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	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)	Herleidbaar wanneer, welke onderdelen/configuraties van de toepassing gewijzigd zijn: - Het is mogelijk om wijzigingen terug te draaien - Naamloze systeemaccounts met uitgebreide rechten zijn toegestaan en (indirect) herleidbaar naar personen - Herleidbaar wanneer de toepassing gewijzigd is - Toegang tot de onderliggende systemen van de toepassing is rolgebaseerd toegewezen - Toegang met root-accounts is gereguleerd, bijvoorbeeld met expliciete notificatie en logging	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	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)

			Maatregelen						
			Integriteit van de gegevens				*Integriteit van de toepassing*		
Integriteit	**Omschrijving**	**Kenmerken**	**Herleidbaarheid (gebruikers)**	**Backup**	**Application controls**	**Onweerlegbaarheid**	**Herleidbaarheid (technisch beheer)**	**Controle integriteit**	**Onweerlegbaarheid (Toepassing)**
Hoog	Integriteit is noodzakelijk. Blijvende juistheid van informatie is noodzakelijk; er zijn geen toleranties toelaatbaar. Het is noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet volledig, correct of actueel is, leidt dit tot ernstige schade.	Bedrijfsproces eist foutloze informatie Gegevens zijn volledig, onbetwistbaar en altijd actueel; Maximaal toegestaan dataverlies na herstel: 4 uur.	Herleidbaar wie, wanneer, welke gegevens gewijzigd heeft: - Gebruikers hebben standaard (by default) niet meer rechten dan nodig: least privilege - Het is mogelijk om wijzigingen terug te draaien - Naamloze gebruikersaccounts zijn niet toegestaan - Herleidbaar wie wanneer de gegevens gewijzigd heeft - Gebruikers hebben geen beheerdersrechten (bijvoorbeeld door aparte accounts) - Wijziging van gegevens is inzichtelijk, waarop tevens signalering ingesteld kan worden voor bv. ongebruikelijke transacties.	Backup is verplicht, minimaal 6 keer per dag, bijvoorbeeld door snapshots. Integriteit van de back-up wordt automatisch bij iedere back-up gecontroleerd. Back-up wordt beschermd door middel van 3-2-1 principe: minimaal drie backup's, op twee verschillende mediatypes waarvan één (kopie) offsite, die offline (niet gekoppeld aan het netwerk) of technisch onaanpasbaar is.	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	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.	Herleidbaar wie, wanneer, welke onderdelen/configuraties van de toepassing gewijzigd heeft: - Het is mogelijk om wijzigingen terug te draaien - Naamloze systeemaccounts met uitgebreide rechten zijn niet toegestaan - Herleidbaar wie wanneer de toepassing gewijzigd heeft - Toegang tot de onderliggende systemen van de toepassing is rolgebaseerd toegewezen. - Rollen geven invulling aan principes 'seggregation of duties' en 'least privilege' - Toegang met root-accounts is streng gereguleerd, bijvoorbeeld door expliciete goedkeuring	Geautomatiseerde controle integriteit toepassing: - De status en werking van patches en updates van firmware en software worden direct gecontroleerd. Bij fouten, vindt actieve signalering van plaats. - Integriteit van de configuratie en software wordt geautomatiseerd gecontroleerd (bijvoorbeeld door hash controles) Maatregelen tegen malware zijn toegepast Secure software development/secure coding guidelines worden toegepast	Gelogd wordt: inlogactiviteit technisch beheer, aanpassingen configuratie en toepassing en overige handelingen van technisch beheer 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 geautomatiseerd gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera) Logging wordt beschermd tegen ongeautoriseerde wijzigingen

			Maatregelen							
			Levenscyclus gegevens	**Logische toegang**	**Fysieke toegang**	**Netwerk toegang**	**Scheiding omgevingen**	**Transport en fysieke opslag**	**Logging**	**Omgaan met kwetsbaarheden**
Vertrouwelijkheid	**Omschrijving**	**Kenmerken**								
Laag	Informatie is voor intern gebruik. Openbaar worden van gegevens leidt tot weinig of geen schade voor een instelling of betrokkene.	Informatie is openbaar of voor intern gebruik. Openbaar worden van gegevens leidt tot weinig of geen schade voor een instelling of betrokkene.	Er wordt invulling gegeven aan wettelijke bewaartermijnen voor persoonsgegevens, logging, leerlingdossiers, et cetera. De applicatie moet het mogelijk maken dat persoonsgegevens verwijderd 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 wordt hergebruikt wordt data gewist.	De toepassing ondersteunt minimaal de volgende maatregelen: - Toegang middels gebruikersnaam en wachtwoord - 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.	Fysieke toegang tot de apparatuur waar de toepassingen en de data verwerkt wordt, is beschermd met minimaal: - Eén factor authenticatie Bezoekers enkel onder begeleiding.	Er is een geïmplementeerd beleid voor netwerktoegang. Daarin zitten minimaal de volgende maatregelen: - Gescheiden netwerken, minimaal op type, bijvoorbeeld WAN/LAN/wifi - Toegang vanuit andere zones is beschermd met aanvullende maatregelen zoals een firewall die poorten dichtzet - Extern benaderbaar door medewerkers en beheerders alleen via beveiligde verbinding met authenticatie en encryptie	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.	Encryptie van transport: - Niet voor intern verkeer - Wel voor extern verkeer, conform de meest recente versie van Uniforme Beveiligingsvoorschriften (UBV) TLS van Edustandaard. Bijvoorbeeld voor koppelingen, mobiele datadragers, cloud, en backups. Voor het gebruik van encryptie wordt gebruik gemaakt van richtlijnen/best practices/standaarden. Bijvoorbeeld van NCSC, ENISA, NIST.	Toegang tot de applicatie (zowel gelukt als mislukt) wordt gelogd. Logging is enkel toegankelijk voor bevoegde personen.	Een risico/dreigingsanalyse zijn uitgevoerd op de toepassing, ter illustratie: - Privacy by design wordt toegepast - OWASP Top 10
Midden	Informatie is vertrouwelijk. De organisatie, instelling of betrokkene kan substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know basis). Hieronder vallen onder andere persoonsgegevens.	Alleen toegankelijk voor direct betrokkenen binnen de organisatie op basis van functie of rol.	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.	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.	Fysieke toegang tot de apparatuur waar de toepassingen en de data verwerkt wordt, is beschermd met minimaal: - Eén factor authenticatie - Logging en monitoring van toegang, bijvoorbeeld cameratoezicht voor de herleidbaarheid. Bezoekers enkel onder begeleiding.	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	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.	Encryptie van transport (zowel voor intern als extern verkeer) is conform de meest recente versie van Uniforme Beveiligingsvoorschriften (UBV) TLS van Edustandaard. Encryptie van opslag, moet minimaal op (virtuele)disk-levelniveau. Hiervoor wordt gebruik gemaakt van richtlijnen/best practices/standaarden, zoals van NCSC, ENISA, NIST.	Toegang tot de applicatie (zowel gelukt als mislukt) en lezen van (persoons) gegevens wordt gelogd. Logging is enkel toegankelijk voor bevoegde personen en toegang ertoe wordt apart gelogd.	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.
Hoog	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.	Toegang is beperkt tot expliciet aangewezen personen binnen de organisatie. Beheerders hebben, waar mogelijk, geen toegang tot de gegevens. Beheerders maken alleen gebruik van persoonlijk herleidbare accounts.	Er wordt invulling gegeven aan wettelijke bewaartermijnen voor persoonsgegevens, logging, leerlingdossiers, et cetera. De applicatie moet het mogelijk maken dat persoonsgegevens verwijderd kunnen worden, bijvoorbeeld op verzoek van de betrokkene. Verwijdering op basis van verstrijken bewaartermijn moet automatisch kunnen. 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). Output van informatie (zoals een printafdruk) met classificatie vertrouwelijk of geheim dient voorzien te zijn van een label.	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.	Fysieke toegang tot de apparatuur waar de toepassingen en de data verwerkt wordt, is beschermd met minimaal: - Twee factor authenticatie - Logging en monitoring van toegang, bijvoorbeeld cameratoezicht voor de herleidbaarheid. Bezoekers enkel onder begeleiding.	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	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.	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.	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.	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.

* Voorbeeld voor regels voor wachtwoorden: zoek op 'NIST Digital Identity Guidelines', ga naar de site van de NIST, open het document 'authentication and lifecycle management', en lees het hoofdstuk 'authenticator and verifier requirements'.