Architectuurkaders

De relevante architectuurkaders voor het examenlogistieke systeem zijn opgenomen in dit document. Elk principe is beschreven in een vaste vorm:

- Een uniek kenmerk en de naam van het principe
- Een toelichting, indien beschikbaar
- Een of meer gevolgen voor het examenlogistiek systeem

De gevolgen zijn nadere uitwerkingen voor de inrichting van het systeem. In de loop van het proces van de keuze en implementatie van het systeem zullen nog meer gevolgen zichtbaar worden. Deze principes zullen worden gebruikt om de oplossingsrichtingen voor inrichtingskeuzes die zichtbaar worden, op te baseren.

In het document wordt verwezen naar brondocumenten waar de principes van mboRijnland in zijn vastgelegd:

- **Basisprincipes Architectuur mboRijnland**
- **Identity en Access Management Architectuurprincipes**
- **Applicatiearchitectuur principes**
- **Informatiebescherming- en privacybeleid**
- **Classificatiekader mboRijnland**
- **Password policy:**
- **BIV-classificatie**

Inhoud

Basisprincipes Architectuur mboRijnland

BP1, mboRijnland stelt de student, zijn leervraag, ontwikkeling en resultaat centraal

Definitie, De student staat centraal en de instelling is gericht op de ontwikkeling van de student.

Gevolg, Bij het inrichten van de logistiek rondom examens wordt uitgegaan van de student journey. De examenlogistiek wordt zo ingericht dat een student zelf zoveel mogelijk in staat wordt gesteld om tijdstip en vorm van examineren te kiezen. De secundaire processen worden gestandaardiseerd en ondersteund met één inrichting van het IV-landschap, waarbij maximaal hergebruik gemaakt wordt van de bestaande voorzieningen.

BP4, De ICT-voorzieningen vergemakkelijken contact en informatievoorziening met en naar studenten, medewerkers en derden

Definitie, mboRijnland wil dat informatie laagdrempelig beschikbaar is voor studenten, medewerkers en derden. Dit vraagt een sterke integratie van digitale diensten. De informatievoorziening moet ook flexibel zijn en snel veranderingen in organisatie en processen kunnen ondersteunen.

Gevolg, de examenlogistiek zal heel waarschijnlijk ondersteund worden door meerdere systemen (Osiris, Xedule, examenlogistiek systeem, afnamesystemen). Goede integratie tussen deze systemen is cruciaal voor een optimale informatievoorziening naar de gebruikers.

BP5, Informatie en services zijn makkelijk te vinden en intuïtief te gebruiken

Definitie, mboRijnland wil studenten snel en gemakkelijk toegang tot alle voor hen relevante informatie bieden - om hiermee hun leerproces optimaal te ondersteunen, wat de kans op studiesucces vergroot.

Gevolg, Studenten worden tijdig en helder geïnformeerd over aankomende examens, behaalde resultaten en inzagerecht, kunnen makkelijk een beroep doen op noodzakelijke voorzieningen voor het maken van examens.

BP6, mboRijnland stimuleert het gebruik van nieuwe digitale ontwikkelingen voor innovatie in het onderwijs

Definitie, mboRijnland wil een bijdrage leveren aan innovatie als permanent proces waar vele partijen in diverse vormen van co-creatie bij betrokken zijn.

Gevolg, De uitwisseling van gegevens in het domein van de examenlogistiek is een cruciale schakel voor het bereiken van de wensen die niet alleen mboRijnland, maar veel andere instellingen ook hebben. mboRijnland ondersteunt standaardisering in dat domein en zet zich in om dit in gezamenlijkheid te ontwikkelen.

BP7, mboRijnland gaat vertrouwelijk om met gegevens en heeft verantwoordelijkheden expliciet belegd

Defnitie, Grenzen van organisaties vervagen en traditionele beveiligingsmaatregelen passen niet meer. MboRijnland zet zich in om op een zorgvuldige manier met gegevens van studenten en medewerkers om te gaan zodat deze niet in handen komen van onbevoegden.

Gevolg,

- Kandidaatgegevens van studenten en medewerkers worden waar mogelijk gepseudonimiseerd verstrekt aan externe partijen bij examenafname.

- Controle op identiteit bij digitale examenafname vindt waar mogelijk plaats aan de hand van (federatieve) authenticatie door mboRijnland.
- Examenresultaten worden gearchiveerd bij mboRijnland volgens doelbinding conform DSP die is gebaseerd op wettelijke vereisten en mboRijnland-specifiek beleid, en externe partijen die examens afnemen vernietigen deze gegevens onmiddellijk na overdracht aan mboRijnland.

Informatie-architectuur principes

IP1, Bedrijfsgegevens hebben een eigenaar

Definitie, Van elk bedrijfsgegeven is duidelijk wie de eigenaar is

Gevolg, het examenlogistieke systeem verwerkt kandidaatgegevens en resultaatgegevens verwerkt, soms op grote schaal (generieke schriftelijke examens). Op elk moment gedurende het proces moet duidelijk zijn welke gegevens worden verwerkt, en voor welk doel. Het architectuurportaal van mboRijnland zal de referentie zijn over wie de eigenaar is en wat de bron is van gegevens die worden verwerkt. Het dataregister van mboRijnland bevat de definitieve informatie over welke gegevens door welke partij worden verwerkt, en met welk doel. Het examenlogistiek systeem zal de gegevens verwerken volgens deze kaders.

IP2, Voor ieder bedrijfsgegeven is (precies) één bron bekend waarin het ontstaat

Definitie, De bron van elk gegevens is duidelijk en vastgelegd. Die bron kan in de loop van de tijd veranderen.

Gevolg, zie IP1

IP4 Bedrijfsgegevens worden alleen in het bronsysteem gewijzigd, aangemaakt en verwijderd

Definitie, De levenscyclus van bedrijfsgegevens wordt bepaald door de gegevenseigenaar en vindt plaats in de bron van de gegevens.

Gevolg, Geconstateerde fouten in examenplanning of –rooster, kandidaat- en resultaatgegevens worden opgelost door correctie in de bron en een nieuwe levering.

IP6, Bedrijfsgegevens hebben een BIV-classificatie

Definitie, Van elk bedrijfsgegeven is duidelijk wat de BIV-classificatie is.

Gevolg, De door het examenlogistieke systeem verwerkte gegevens hebben een BIV classificatie (bijgevoegd de BIV classificatie voor de gegevensstromen Examenkandidaten en Resultaatgegevens).

IP9 Integrale informatievoorziening

Definitie Alle bedrijfsgegevens worden uniform en ondubbelzinnig met elkaar in verband gebracht zodat er een overkoepelend inzicht ontstaat over alle bedrijfsgegevens en de daaruit volgende informatie.

Gevolg, de bronsystemen van mboRijnland leveren identificerende gegevens voor student (pseudoniem), examen, afnamemoment en andere relevante entiteiten. Digitale examenafnamesystemen leveren deze gegevens ongewijzigd terug bij het aanleveren van de resultaten. Het examenlogistiek systeem verwerkt de identificerende gegevens ongewijzigd.

IP10, Studenten, docenten/medewerkers kunnen alle benodigde informatie vanaf één punt vinden

Definitie, Er is één plek waar belanghebbenden de informatie kunnen vinden die ze nodig hebben voor hun werkzaakheden.

Gevolg, Studenten, examinatoren en begeleiders zien de planning en het rooster van alle examens die voor hen van belang zijn in het examenlogistieke systeem.

Identity en Access Management Architectuurprincipes

IAM1, Toegang tot IT-systemen wordt geauthentiseerd en geautoriseerd

Definitie, Gebruikers mogen uitsluitend toegang hebben tot gegevens of functionaliteit waartoe zij zijn geautoriseerd. Het voorkomen van ongeautoriseerde toegang vraagt maatregelen in alle betrokken IT-systemen.

Gevolg, Toegang tot de functionaliteit voor examens in de examenlogistieke- en de afnamesystemen is alleen maar mogelijk na authenticatie. Authenticatie vindt plaats aan de hand van de door mboRijnland hebruikte SurfConext of de eigen authenticatievoorziening van mboRijnland (AD Federatie). Functionaliteiten mogen worden gebruikt op basis van (rol-gebaseerde) autorisatie. Automatische uitwisseling van informatie is adequaat beveiligd (zie IAM12: Beveiligingsmaatregelen zijn gebaseerd op het risicoprofiel).

IAM2, Identiteiten, rollen en grofmazige autorisaties worden centraal geadministreerd

Definitie, Centrale administratie van identiteiten en grofmazige autorisaties zorgt ervoor dat er centraal zicht is op identiteiten, dat functiescheidingsregels kunnen worden gecontroleerd en dat gebruik van applicaties kan worden herleid naar specifieke gebruikers.

Gevolg, provisioning van medewerkergegevens en hun autorisaties in het examenlogistiek systeem wordt zoveel mogelijk gecentraliseerd.

IAM3, Gebruikers-accounts hebben een eigenaar

Definitie, Door een eigenaar toe te kennen aan elk account dat mboRijnland uitgeeft is er altijd een aanspreekpunt dat kan aangeven of toegang nog wenselijk is.

Gevolg, voor interactieve gebruikers en voor de automatische uitwisselingen van het examenlogistieke systeem zijn gebruikersaccounts gemaakt, die allemaal aan een medewerker of student gekoppeld zijn.

IAM4, Wachtwoorden conformeren aan de password policy van mboRijnland

Definitie, Door het definiëren van een policy voor wachtwoorden worden de belangrijkste risico's rondom het misbruiken van wachtwoorden voorkomen.

Gevolg, Authenticatie van gebruikers vindt bij voorkeur plaats op basis van SSO waarbij SurfConext of de authenticatieserver van mboRijnland gebruikt wordt (zie IAM1). Alleen als dat echt niet mogelijk is, kunnen eigen accounts in het examenlogistiek systeem gemaakt worden, maar dan geldt dat dit systeem de password policy van mboRijnland afdwingt.

IAM6, De autorisaties van de bronapplicatie zijn leidend

Definiete, Naast de applicatie die is aangewezen als bron-applicatie kunnen portalen, zoekmachines en andere applicaties een alternatieve ingang bieden tot gegevens. Het is belangrijk om bij deze alternatieve ingang te bewaken dat de autorisaties in het bronsysteem gehandhaafd blijven en ongeautoriseerde toegang tot bepaalde gegevens wordt voorkomen.

Gevolg, De soorten gegevens die verwerkt worden in de examenketen zijn in kaart gebracht, er is een eigenaar aan toe gekend en er zijn autorisaties voor gebruik beschreven. Het examenlogistiek systeem ondersteunt de verwerking van de gegevens volgens deze autorisaties.

IAM7, Toegang tot autorisatieobjecten is rol-gebaseerd

Definitie, Door autorisaties te baseren op de rol van de gebruiker hoeven autorisaties niet op individueel niveau te worden toegekend, waardoor autorisatiebeheer efficiënter kan plaats vinden.

Gevolg, Systemen in de examenketen gebruiken rol-gebaseerde autorisatie. De rollen zijn afkomstig uit de provisioning van gebruikers (principe IAM2: Identiteiten, rollen en grofmazige autorisaties worden centraal geadministreerd).

IAM8, **Toegangsrechten zijn gebaseerd op wat nodig is voor het uitoefenen van de functie**

Definitie, mboRijnland geeft gebruikers precies die (minimale) rechten die zij nodig hebben voor het uitoefenen van hun functie. Dit gaat zoveel mogelijk rol-gebaseerd (Principe IAM7: Rol-gebaseerde Autorisatie).

Gevolg: mboRijnland brengt in kaart welke rollen welke autorisaties nodig hebben. Het examenlogistiek systeem ondersteunt deze indeling.

IAM9, Autoritatieve bronnen en doelsystemen worden aangesloten middels een provisioningsysteem en bijbehorende connectoren

Definitie, Een geautomatiseerde uitwisseling van gebruikersgegevens en –rollen via een provisioningsysteem voorkomt handmatige acties die inefficiënt en foutgevoelig zijn.

Gevolg, het examenlogistiek systeem ondersteunt invoer en verwijdering (of deactiviering) van gebruikersgegevens via een automatische koppeling en – bij voorkeur – een relevante standaard zoals SCIM.

IAM10, Gebruik van systemen en toegang tot gegevens is herleidbaar naar gebruikers

Definitie, Bij fouten, misbruik of fraude moet het mogelijk zijn om te achterhalen wie bepaalde handelingen heeft uitgevoerd, zodat de gebruiker kan worden aangesproken en verantwoordelijk kan worden gesteld.

Gevolg, Het examenlogistiek systeem logt het gedrag van alle gebruikers, inclusief beheerders. Het gaat hierbij zowel om het aanbrengen van wijzigingen als om het lezen of downloaden van gegevens.

IAM11, Beveiligings-gerelateerde gebeurtenissen worden vastgelegd in een centrale log

Definitie, Door de logging op een centraal punt bijeen te brengen ontstaat een heldere blik op alle informatie vanuit de verschillende componenten uit de infrastructuur en kunnen correlaties gelegd worden.

Gevolg, Het examenlogistiek systeem koppelt de logs aan de centrale log-server van mboRijnland.

IAM12, Beveiligingsmaatregelen zijn gebaseerd op het risicoprofiel

Definitie, De risicoclassificatie van informatie bepaalt welke maatregelen moeten worden genomen om de integriteit en vertrouwelijkheid van de informatie te bewaken.

Gevolg, Voor alle gegevensstromen in de examenketen is een BIV-classificatie opgesteld (zie IP6). Het examenlogistiek systeem is voor het verwerken van deze gegevens beveiligd met maatregelen die gekoppeld zijn aan de betreffende risico-klasse.

IAM13, Applicaties zijn federatief toegankelijk voor gebruikers waarmee mboRijnland geen vastgelegde relatie heeft

Definitie, Steeds meer gebruikers van applicaties van mboRijnland zijn afkomstig zijn van andere organisaties, bijvoorbeeld bedrijven waarmee mboRijnland samenwerkt in het kader van hybride onderwijs. Het is onwenselijk al deze gebruikers vast te leggen in de directory van mboRijnland.

Gevolg, Het systeem voor examenlogistiek ondersteunt toegang voor gebruikers van buiten mboRijnland door middel van SSO via SurfConext of de authenticatieserver van mboRijnland gebruikt wordt (zie IAM1).

Applicatiearchitectuur principes

AA2, Data wordt beheerd en bewerkt in daartoe aangewezen bronapplicaties. Informatie wordt geleverd aan informatiegebruikers via die datalaag

Definitie, Het doel van de applicatie architectuur is dat de mogelijkheid van levering van gegevens door de applicaties niet beperkend is in de behoefte van gegevens levering aan de afnemer.

Gevolg, Uitwisseling van gegevens door het examenlogistieke systeem wordt ingericht via de datalaag, behalve als er door de leverancier van het systeem beheerde koppelingen bestaan die de gewenste uitwisseling ondersteunen.

AA3, Van relevante gebeurtenissen wordt een registratie bijgehouden

Definitie, Registratie van relevante gebeurtenissen helpt bij inzicht in de (status van) verwerking binnen de keten.

Gevolg, (zie ook IAM10) Systemen in de examenketen loggen het gedrag van alle gebruikers, inclusief beheerders. Het gaat hierbij zowel om het aanbrengen van wijzigingen als om het lezen of downloaden van gegevens.

Informatiebeschermings- en privacybeleid

IBP3, **Bij mboRijnland is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen.**

Gevolg: Doel en grondslagen van alle uitwisselingen van persoonsgegevens in de examenlogistieke keten is expliciet gemaakt en vastgelegd.

IBP8, mboRijnland classificeert informatie en informatiesystemen.

Gevolg: (zie ook IP6, IAM12) Voor alle gegevensstromen in de examenketen die door het examenlogistiek systeem worden verwerkt, wordt een BIV-classificatie opgesteld. Het examenlogistiek systeem wordt beveiligd met maatregelen die gekoppeld zijn aan de betreffende risico-klasse.

IBP9, **mboRijnland sluit met alle leveranciers van digitale onderwijsmiddelen verwerkersovereenkomsten af als zij persoonsgegevens verwerken.**

Gevolg, Met eventuele nieuwe leveranciers van het examenlogistiek systeem worden, voor zover in dat systeem persoonsgegevens worden verwerkt, verwerkersovereenkomsten afgesloten.

IBP13, mboRijnland neemt passende organisatorische of technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren

Gevolg, mboRijnland zal met de leverancier van het examenlogistiek systeem afspraken maken waarmee de performance van de leverancier op deze doelen meetbaar gemaakt wordt, gemeten wordt zodat handhaving hierop mogelijk is

IBP14, mboRijnland zal alle beveiligingsincidenten en datalekken vastleggen

Gevolg, de leverancier van het examenlogistiek systeem beschikt over bescherming tegen en monitoring van beveiligingsincidenten en datalekken, en informeert mboRijnland over gebeurtenissen op dit vlak met gegevens van mboRijnland.

IBP15, mboRijnland kiest ten aanzien van informatiebeveiliging (autorisatie en authenticatie) voor de vooronderstelling "Alles is in principe verboden tenzij het uitdrukkelijk is toegelaten"

Gevolg, (zie ook IAM8) Het examenlogistiek systeem beschikt over een systeem van autorisaties dat op deze manier kan worden ingericht.

Classificatiekader mboRijnland

Classificatie geeft een inschatting van de gevoeligheid en het belang van de data om tot een juiste mate van beveiliging te komen. Niet alle data zijn even vertrouwelijk of moeten bij een incident even snel weer beschikbaar te zijn.

Het classificatiekader is opgesteld om te komen tot een manier van indelen van de gevoeligheid van informatie en informatiesystemen op een betrouwbare en herhaalbare manier. Classificatie gebeurt op drie kwaliteitscriteria: beschikbaarheid, integriteit en vertrouwelijkheid.

- **Beschikbaarheid**: de mate waarin de beschikbaarheid en ongestoorde voortgang van de ICT-dienstverlening gewaarborgd wordt.
- **Integriteit**: de mate waarin de juistheid, volledigheid en tijdigheid van de IT-dienstverlening gewaarborgd wordt.
- **Vertrouwelijkheid**: de mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.

CK3, **Er wordt gestreefd naar een verantwoord, maar zo passend mogelijk classificatieniveau**

Gevolg,

De classificaties die mboRijnland hanteert zijn:

- Beschikbaarheid
    - Midden: de hersteltijd is maximaal 24 uur voor servers, applicaties en data en 48 uur voor het netwerk.
    - Hoog: de hersteltijd is maximaal 8 uur voor servers, applicaties en data en 24 uur voor het netwerk
- Integriteit
    - Laag: Volledigheid: Alle gevraagde data zijn ingevuld
    - Midden: Volledigheid en Juistheid. Juistheid: Een medewerker van mboRijnland controleert of de gegevens juist zijn.

    - Hoog: Volledigheid, Juistheid en Actualiteit. Actualiteit: medewerkers van mboRijnland toetsen of de gegevens actueel zijn.
- Vertrouwelijkheid
    - Laag: toegang op basis van aanstellingsovereenkomst tot diensten en faciliteiten (netwerk, e-mail, etc.).
    - Midden: toegang op basis van rol of functie.
    - Hoog: toegang op naam op basis van persoonlijke rechten.

BIV classificaties

De BIV classificatie van de gegevensstroom “Kandidaatgegevens” is MMM. De BIV classificatie van de gegevensstroom “Resultaatgegevens” is MMM (zie bijlagen voor de BIV classificaties inclusief toelichting). De maatregelen waar het examenlogistiek systeem aan moet voldoen om de verwerking deze gegevensstromen adequaat te beveiligen zijn geformuleerd in het modelbestand van de BIV classificatie van Bureau Edustandaard. Onderstaande maatregelen zijn de maatregelen die gelden voor de genoemde classificaties (MMM). Waar onderstaande maatregelen overlappen in strekking met bovenstaande principes van mboRijnland zelf, geldt de formulering van mboRijnland. Mochten onderstaande maatregelen conflicteren met bovenstaande principes, dan moet van geval tot geval worden bepaald hoe hiermee om wordt gegaan, maar in beginsel prevaleren de principes van mboRijnland.

Maatregelen op het gebied van beschikbaarheid

BM1. Ontwerp

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.

BM2. Capaciteit beheer

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.

BM3. Onderhoud

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.

BM4. Testen

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.

BM5. Monitoring

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.

BM6. Herstel

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.

Maatregelen op het gebied van integriteit

IM1. Herleidbaarheid (gebruikers)

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.

IM2. Backup

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.

IM3. Application controls

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

IM4. Onweerlegbaarheid

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)

IM5. Herleidbaarheid (technisch beheer)

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

IM6. Controle integriteit

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

IM7. Onweerlegbaarheid (Toepassing)

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 op het gebied van vertrouwelijkheid

VM1. Levenscyclus gegevens

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.

VM2. Logische toegang

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.

VM3. Fysieke toegang

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.

VM4. Netwerk toegang

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

VM5. Scheiding omgevingen

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.

VM6. Transport en fysieke opslag

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.

VM7. Logging

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.

VM8. Omgaan met kwetsbaarheden

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.