

Informatie architectuur principes KW1C

Dit overzicht aan informatie-architectuurprincipes is een selectie uit de architectuurprincipes van het Koning Willem I College. De principes dienen door aanbieders te worden onderschreven.

Classificatie: intern

Intellectueel eigendom van het Koning Willem I College. Verdere verspreiding uitsluitend met toestemming van het KW1C.



Principe nummer	1.4	(23)
Versie	4.0	
Titel	Toegang tot de informatievoorziening	
Principe	Gebruikers krijgen toegang tot delen van de KW1C-informatievoorziening afhankelijk van moment, locatie en apparaat.	
Rationale	Gebruikers van de informatievoorziening van KW1C werken naast door KW1C beheerde apparaten deels of helemaal op eigen apparaten, binnen of buiten het college. De informatievoorziening moet daarom in een beveiligde omgeving ontsloten kunnen worden op die apparaten. Eigen devices maken het risico op datalekken groter. Dit vergt maatregelen als devicemanagement en / of extra bescherming door middel van moderne authenticatie.	
Implicaties	<ol style="list-style-type: none">1. KW1C stelt eisen aan het veilig gebruik van meegebrachte apparaten en extern gebruik van de informatievoorziening. Gebruikers conformeren zich impliciet aan de gestelde eisen.2. Gebruikers krijgen toegang tot (delen) van de informatievoorziening via de eigen meegenomen apparaten.3. Applicaties zijn web gebaseerd of worden via web gebaseerde technologie zoals een virtuele werkplek of applicatie aangeboden.4. Breed beschikbaar gestelde applicaties behoren op elk apparaat te kunnen worden gebruikt, inclusief mobiele telefoons en tablets.	
Uitzonderingen	Niet van toepassing	

Principe nummer	1.7	(4)
Versie	3.0	
Titel	Bescherming persoonsgegevens	
Principe	Met informatie en documenten wordt integer en vertrouwelijk gewerkt.	

Rationale Privacy is een essentieel recht van alle betrokkenen bij KW1C. We beschouwen gegevens van studenten en medewerkers als kostbaarheden, die wij binnen de organisatie in bruikleen hebben.

Implicaties

1. Het Koning Willem I College hanteert een informatie-beveiligings- en privacybeleid dat ten minste voldoet aan relevante wet- en regelgeving. Het opvragen, registreren, gebruiken, ontsluiten, bewaren en vernietigen van informatie en documenten gebeurt op basis van dit informatiebeveiligings- en privacybeleid.
2. Projecten, implementaties en applicaties met een informatiecomponent houden rekening met vastgestelde eisen op het gebied van informatiebeveiliging en privacy.
3. Gegevens en systemen zijn door proces-, systeem- en data-eigenaren geclassificeerd volgens een BIV-classificatie.
4. Het Koning Willem I College hanteert een documentmanagementbeleid. Op basis van dit beleid zijn de processen en systemen ten behoeve van het beheer van (digitale) documenten en het archief ingericht
5. De informatievoorziening is uit oogpunt van informatiebeveiliging voor gebruikers uitsluitend benaderbaar met Multi Factor Authenticatie (zie ook principe 3.7).
6. Ook voor toegang tot applicaties via telefoon is er een 'beveiligde omgeving' waarbij toegang op afstand door KW1C geregeld kan worden.

Uitzonderingen Niet van toepassing

Principe nummer	1.9	(19)
Versie	2.0	
Titel	Huisstijl	
Principe	Informatiepublicaties worden in de huisstijl van het KW1C gepubliceerd.	

Rationale De huisstijl is van belang voor een eenduidige uitstraling en daarmee herkenbare uitstraling van de organisatie naar alle stakeholders, zowel intern als extern.

Implicaties

1. De informatievoorziening van het KW1C wordt gepresenteerd in de huisstijl van het college conform de richtlijnen uit het huisstijlhandboek.
2. Applicaties en applicatiecomponenten als zelfservice en rapportages zijn bij voorkeur te presenteren in de huisstijl, maar kunnen op zijn minst worden voorzien van het KW1C-logo.

Uitzonderingen Niet van toepassing

Principe nummer	1.10	(24)
Versie	2.0	
Titel	De informatievoorziening is Nederlandstalig	
Principe	De informatievoorziening is Nederlandstalig.	

Rationale	Het gebruik van applicaties moet in de Nederlandse taal mogelijk zijn.
-----------	--

Implicaties	1. Leveranciers zorgen voor een mogelijkheid dat de applicatie in het Nederlands gebruikt kan worden. 2. Bij voorkeur heeft het KW1C de mogelijkheid om in een applicatie zelf definities en omschrijvingen voor termen te definiëren.
-------------	---

Uitzonderingen	Sommige systemen kunnen vanwege het gebruik (talenonderwijs) in andere talen beschikbaar worden gesteld.
----------------	--

Principe nummer	1.11	(57)
Versie	1.0	
Titel	Duurzaamheid	
Principe	KW1C streeft naar duurzame oplossingen op IT-gebied.	

Rationale	KW1C heeft duurzaamheid hoog in het vaandel staan en wil dat uitdragen naar toeleveranciers.
-----------	--

Implicaties	Bij iedere vernieuwing in de informatievoorziening is de duurzaamheid van de oplossing een criterium in de keuze.
-------------	---

Uitzonderingen	Niet van toepassing
----------------	---------------------

Principe nummer	2.1	(32)
Versie	4.0	
Titel	Eén bron	
Principe	Elk gegeven kent één proces en één bronsysteem waarin het gegeven wordt vastgelegd en beheerd.	
Rationale	Het vastleggen en onderhouden van een gegeven in één bronapplicatie is een voorwaarde om de betrouwbaarheid en integriteit van dat gegeven te kunnen garanderen. Het vastleggen van de definitie en eigenschappen van een KW1C-gegeven in een centraal KW1C-Informatiemodel garandeert dat de informatievoorziening / -verstrekking op basis van dat gegeven eenduidig, betekenisvol en juist is en dat de betekenis overeenkomt met de definities uit de bedrijfsprocessen.	
Implicaties	<ol style="list-style-type: none"> 1. Van elk gegeven is bekend in welk proces en in welk bronsysteem het wordt geregistreerd. 2. Van elk gegeven is bekend wie de gegevenseigenaar is. Dit is in de regel de proceseigenaar van het proces waarin het gegeven wordt geregistreerd en onderhouden. 3. Elk gegeven waarover gerapporteerd moet worden of dat gebruikt wordt in een ander systeem is als (eigenschap van een) entiteit in het logische KW1C-gegevensmodel opgenomen, elke entiteit is als datacomponent opgenomen in het KW1C-integratieplatform. 	
Uitzonderingen	Niet van toepassing	

Principe nummer	2.2	(64)
Versie	1.0	
Titel	Data digitaal aanleveren	
Principe	Gegevens worden digitaal aangeleverd.	
Rationale	Als data bij de bron al digitaal wordt aangeleverd biedt dat mogelijkheden voor het (verder) digitaliseren van processen. Het biedt ook meer mogelijkheden om de kwaliteit van de data al bij de bron te controleren, waardoor de datakwaliteit wordt verbeterd.	
Implicaties	<ol style="list-style-type: none"> 1. Gebruikers kunnen gevraagde informatie digitaal aanleveren. 2. Gebruikers kunnen eigen gegevens controleren, aanvullen of verbeteren via een selfservice mogelijkheid (zie ook principe 1.10) 	
Uitzonderingen	Niet van toepassing	

Versie 1.0

Titel Gestandaardiseerde gegevensuitwisseling

Principe **De uitwisseling van gegevens is gestandaardiseerd.**

Rationale Standaardisatie van informatie-uitwisseling vergemakkelijkt vervanging van systemen en het aansluiten van nieuwe systemen op de informatie-infrastructuur. Via een integratieplatform wordt alle informatie tussen systemen uitgewisseld zodat voor ieder systeem slechts 1 interface (of 1 set interfaces) onderhouden hoeft te worden in plaats van vele point-to-point interfaces.

Implicaties De inrichting van de informatievoorziening wordt waar mogelijk gebaseerd op een Service Oriented Architecture, waarbij de uitwisseling van gegevens zoveel mogelijk via standaard services verloopt.

Uitzonderingen Niet van toepassing

Versie 3.0

Titel Gegevens naar de KW1C integratielaag

Principe **Gegevens uit bronsystemen worden gerepliceerd naar de KW1C-integratielaag zodat het KW1C die gegevens vanuit het integratieplatform beschikbaar kan stellen aan de KW1C Informatievoorziening.**

Rationale In de integratielaag kunnen gegevens uit verschillende bronsystemen worden gecombineerd, verrijkt en worden voorzien van bedrijfsregels, die niet in de bronsystemen zijn opgenomen. Het zorgt voor een ontkoppeling tussen bronsysteem en afnemende systemen (bronsysteem onafhankelijk applicatielandschap). Daarnaast vormen de gegevens in de integratielaag een belangrijke bron voor data-analyses.

Implicaties

1. Leveranciers van bronsystemen faciliteren de replicatie van gegevens naar de KW1C-integratielaag.
2. Leveranciers verstrekken een database-datamodel of een gegevensmodel van die entiteiten in de applicatie, die deel uit (gaan) maken van het KW1C-informatiemodel. De informatie is voorzien van adequate metadata en documentatie.
3. Het maken van een datakopie gebeurt voor een aantal door KW1C nader te benoemen processen door middel van near-realtime replicatie vanuit de bronsystemen.
4. Voor applicaties aanwezig in het KW1C datacenter (ook te noemen on-premise) geldt, dat de near-real-time kopie van brondatabase aangeleverd dient te zijn van de soort Microsoft SQL Server.
5. Voor applicaties buiten het KW1C datacenter geldt, dat de replicatie gebeurt op basis van óf database-replicatie, óf op basis van push& pull (volgens het publish & subscribe-principe)

Uitzonderingen

Principe nummer	2.5	(42)
-----------------	-----	------

Versie	3.0
--------	-----

Titel	Bewaartermijn gegevens
-------	------------------------

Principe	Applicaties hebben voorzieningen om wettelijke of door KW1C vastgestelde bewaar- of vernietigingstermijnen te hanteren.
----------	--

Rationale	Wettelijke regels geven minimale en maximale bewaartermijnen van gegevens en documenten aan.
-----------	--

Implicaties	1. Applicaties hebben functionaliteiten om bewaar- en vernietigingstermijnen te kunnen handhaven, ook wanneer die termijnen gebaseerd zijn op een nog vast te stellen datum. 2. Onder vernietigen wordt ook het anonimiseren verstaan.
-------------	---

Uitzonderingen	Niet van toepassing
----------------	---------------------

Principe nummer	2.6	(35)
-----------------	-----	------

Versie	4.0
--------	-----

Titel	KW1C als verantwoordelijke voor brongegevens
-------	--

Principe	Het KW1C is verantwoordelijk voor alle gegevens die KW1C verwerkt in systemen.
----------	---

Rationale	Het KW1C is verantwoordelijk voor een goede informatievoorziening en daarmee voor de gegevens in de bronsystemen. Het KW1C moet vanuit die verantwoordelijkheid ook verantwoording afleggen over deze gegevens in de informatievoorziening. Dat kan alleen, als het KW1C ten alle tijde kan beschikken over brongegevens als ook over de context van die brongegevens in de vorm van een goede documentatie en/of een datamodel. De verantwoordelijkheid houdt ook in, dat KW1C <i>verwerkingsverantwoordelijke</i> is voor alle persoonsgegevens in de zin van de AVG.
-----------	---

Implicaties	1. Leveranciers van informatiesystemen faciliteren de registratie, opslag, verwerking en presentatie van gegevens in hun systeem maar hebben alleen toegang tot die gegevens op basis van een verwerkersovereenkomst van het KW1C voor specifiek benoemde werkzaamheden waarin afspraken zijn gemaakt over die toegang. 2. Leveranciers stellen brongegevens uit hun informatiesysteem beschikbaar in een voor het KW1C begrijpelijke context. 3. Leveranciers stellen een overzicht van functionele brongegevens in hun applicatie met actuele definities beschikbaar aan het KW1C. 4. Leveranciers mogen de gegevens niet voor andere dan door KW1C vastgestelde doeleinden verwerken. Dit wordt vastgelegd in een door het KW1C goedgekeurde verwerkersovereenkomst. 5. Functioneel beheerders van het KW1C hebben voor controledoeleinden rechtstreeks (leesrechten-) toegang tot de KW1C-data van het bronsysteem.
-------------	---

Uitzonderingen	Niet van toepassing
----------------	---------------------

Versie 3.0

Titel Verantwoordelijkheid voor juiste AVG-document-classificatie

Principe **De eigenaar van een geautomatiseerd samengestelde publicatie is verantwoordelijk voor de juiste documentclassificatie. De publicatie-eigenaar stemt van te voren af met de data-eigenaren.**

Rationale Om aan wet- en regelgeving te kunnen voldoen, is het noodzakelijk dat elke informatie-publicatie geclassificeerd is. Een classificatie informeert gebruikers hoe hij of zij met het document, bestand of gegevensset moet omgaan. Ook kunnen er technische maatregelen gebaseerd worden op de classificatie om datalekken te voorkomen.

Implicaties

1. Elke gegevensgebaseerde informatiepublicatie kent een classificatie volgens een KW1C-standaard.
2. Rapport- en data-eigenaren zijn verantwoordelijk voor het vaststellen van die classificatie. Wie dat is wordt vastgelegd in het FO van die informatie-publicatie.
3. Zonder vastgestelde classificatie wordt de publicatie niet naar productie gebracht.
4. Informatiesystemen die geautomatiseerd samengestelde publicaties kunnen genereren, kunnen omgaan met de door het KW1C vastgestelde classificatie van documenten en gegevensbronnen.

Uitzonderingen Niet van toepassing

Versie 1.0

Titel Archivering

Principe **Archiefwaardige informatie wordt in aangewezen applicaties gearchiveerd**

Rationale Onderwijsinstellingen voeren een aantal openbaar gezagtaken uit en hebben daardoor vanuit de archiefwet een verplichting bepaalde informatie blijvend te bewaren of te vernietigen na een bepaalde periode. Daarnaast hebben onderwijsinstellingen ook andere verplichtingen naar stakeholders en de maatschappij om bepaalde informatie te bewaren.

Implicaties

1. Er is een instellingspecifiek Document Structuur Plan (DSP) waarin alle formele soorten documenten, hun bewaartermijn en/of vernietigingstermijn zijn beschreven.
2. Gegevens worden beheerd in de daarvoor aangewezen applicaties zodat zij op een later moment kunnen worden gereproduceerd.
3. Te archiveren documenten die niet expliciet worden beheerd en gearchiveerd in een specifieke applicatie worden in een duurzaam formaat opgeslagen in een document management systeem met record management functionaliteit.
4. Gegevens die lang bewaard moeten worden blijven leesbaar doordat de daarvoor noodzakelijke apparatuur en programmatuur wordt bewaard of doordat ze worden omgezet in een ander formaat.
5. Persoonsgegevens worden na de bewaartermijn waar mogelijk geanonimiseerd bewaard.

Uitzonderingen De AVG verstaat onder verwijderen ook anonimiseren. Waar persoonsgegevens kunnen worden geanonimiseerd heeft dat de voorkeur boven het daadwerkelijk verwijderen.

Principe nummer	3.3	(60)
Versie	1.0	
Titel	Cloud	
Principe	Cloudoplossingen prevaleren boven het zelf hosten van oplossingen	

Rationale	Cloudoplossingen vergen minder eigen voorzieningen en beheer.
-----------	---

Implicaties	<ol style="list-style-type: none">1. Bij nieuwe applicaties wordt in eerste instantie gekeken naar beschikbare Cloud oplossingen.2. Leveranciers dienen verwerkersovereenkomsten af te sluiten, te beschikken over de juiste beveiligingscertificaten en mee te werken aan privacy impact assessments.
-------------	---

Uitzonderingen	Niet van toepassing
----------------	---------------------

Principe nummer	3.4	(59)
Versie	1.0	
Titel	Open standaarden	
Principe	Applicaties ondersteunen open standaarden.	

Rationale	Alle aan te schaffen applicaties dienen de geldende open standaarden voor uitwisseling van data of toegang tot de applicatie te ondersteunen. Ontbreken van standaarden of het gebruik van eigen standaarden bevorderen vendor lock-in en bemoeilijken data-uitwisseling met andere applicaties. Open standaarden bevorderen de integreerbaarheid. Voorbeelden zijn LDAP, PDF, HTML, XML, etc.
-----------	--

Implicaties	<ol style="list-style-type: none">1. Applicaties die alleen proprietary (eigen) standaarden ondersteunen worden niet aangeschaft.2. KW1C onderhoudt een lijst met gebruikte open standaarden binnen de architectuur.
-------------	---

Uitzonderingen	Niet van toepassing
----------------	---------------------

Principe nummer	3.5	(9)
-----------------	-----	-----

Versie	1.0
--------	-----

Titel	Beveiliging
-------	-------------

Principe	Alle informatiesystemen en (digitale) gegevensbestanden voldoen aan het informatiebeveiligingsbeleid van KW1C.
----------	---

Rationale	KW1C heeft een informatiebeveiligingsbeleid waarin is vastgelegd hoe wordt omgegaan met informatiesystemen en digitale gegevensbestanden.
-----------	---

Implicaties	<ol style="list-style-type: none">1. Leveranciers kunnen door middel van erkende certificeringen aantonen dat systemen en procedures voldoen aan het informatiebeveiligingsbeleid van het KW1C.2. Indien bronsystemen persoonsgegevens bevatten, kunnen leveranciers aantonen dat zij ISO 27001 gecertificeerd zijn.3. Alle gegevenstransportverbindingen (voor de applicatie en real-time replicatie en informatieverstrekking) voldoen aan de bepalingen uit het managementsysteem (ISMS) en betreffende beheersmaatregelen van ISO 27001.4. Het systeem moet aangesloten kunnen worden op het KW1C Identity-& Accessmanagement Systeem (SmartAIM) om aan te kunnen sluiten bij het centrale rollen- en autorisatiebeheer van het KW1C.5. Systemen, waarin persoonsgegevens worden opgeslagen of worden geraadpleegd, kunnen voor toegang en gebruik overweg met Multi Factor Authenticatie.
-------------	--

Uitzonderingen	Niet van toepassing
----------------	---------------------

Principe nummer	3.6	(8)
-----------------	-----	-----

Versie	2.0
--------	-----

Titel	Moderne authenticatie
-------	-----------------------

Principe	Toegang tot niet publieke informatie vindt altijd plaats op basis van moderne authenticatie ter identificatie bij KW1C.
----------	--

Rationale	Toegang tot informatie, gegevens, processen en systemen vereist een betrouwbare identiteit. Het niveau van noodzakelijk vertrouwen in de identiteit is afhankelijk van de risicoclassificatie en wordt daar waar nodig afgedwongen met meervoudige authenticatie.
-----------	---

Implicaties	<ol style="list-style-type: none">1. Gebruikers dienen zich voor toegang tot systemen te identificeren op een wijze waarop de identiteit van de gebruiker kan worden gevalideerd door KW1C.
-------------	---

*Als gebruikers zien wij medewerkers, studenten, beheerders en gasten.

Uitzonderingen	Niet van toepassing
----------------	---------------------

Principe nummer	3.7	(10)
-----------------	-----	------

Versie	4.0
--------	-----

Titel	Seamless Single Sign On
-------	-------------------------

Principe	Een KW1C gebruiker krijgt op basis van één login toegang tot alle KW1C-informatievoorziening.
----------	--

Rationale	Seamless single sign-on vergroot het gebruiksgemak van toegang tot de diverse systemen binnen de KW1C-informatievoorziening. (Zie bron)
-----------	--

Implicaties	1. KW1C hanteert internationaal erkende standaarden t.a.v. SSSO. Deze standaarden en eisen zijn daarmee op de gehele KW1C-informatievoorziening van toepassing. 2. Technisch moet het seamless single sign-on-principe ingericht worden door gebruik te maken van moderne authenticatie."
-------------	--

Uitzonderingen	Niet van toepassing
----------------	---------------------

Principe nummer	3.8	(14)
-----------------	-----	------

Versie	2.0
--------	-----

Titel	Domeinnaam van webapplicaties
-------	-------------------------------

Principe	Alle webapplicaties zijn voorzien van een KW1C (sub-)domeinnaam.
----------	---

Rationale	Voor gebruikers van KW1C web applicaties dient duidelijk te zijn dat van officiële en/of door Koning Willem I College ondersteunde webapplicaties gebruik gemaakt wordt.
-----------	--

Implicaties	1. Formaten die zijn toegestaan: https://zzzz.kw1c.nl https://yyyy.xxxx.kw1c.nl 2. De te gebruiken domeinnaam is voorzien van de naam van het proces dat wordt ondersteund door de webapplicatie. De domeinnaam bevat niet de naam van de leverancier of applicatie.
-------------	--

Uitzonderingen	Niet van toepassing
----------------	---------------------

Principe nummer	3.9	(15)
Versie	2.0	
Titel	Webapplicaties en certificaten	
Principe	Applicaties aangeboden via intra- en internet voldoen aan actuele en internationaal erkende en geaccordeerde standaarden.	
Rationale	De continuïteit en veiligheid van webapplicaties dienen maximaal gegarandeerd te zijn. Dat kan alleen als er gebruik gemaakt wordt van actuele en internationaal erkende en geaccordeerde standaarden.	
Implicaties	<ol style="list-style-type: none">1. Webapplicaties dienen te voldoen aan actuele en internationaal erkende standaarden op gebied van beveiliging.2. Webapplicaties zijn beveiligd (SSL, HTTPS://).3. Beveiligde verbindingen maken gebruik van één certificaat per geregistreerd (sub)domein.	
Uitzonderingen	Niet van toepassing	

Principe nummer	3.10	(13)
Versie	3.0	
Titel	Releases	
Principe	Een leverancier meldt wijzigingen in een bronsysteem minimaal binnen een afgesproken termijn voor productie-release.	
Rationale	Er is tijd nodig om de impact te bepalen van wijzigingen op het KW1C-informatiemodel en eventuele interfaces.	
Implicaties	<ol style="list-style-type: none">1. Major releases worden minimaal 3 maanden van te voren door de leverancier aangekondigd.2. Minor releases (patches) worden minimaal één week voor productiedatum aangekondigd.3. Kleine databasewijzigingen worden minimaal 2 weken vooraf aangekondigd.4. Releases worden eerst beschikbaar gesteld op een test- of acceptatieomgeving.5. Releases zijn altijd voorzien van duidelijke releasenotes.6. Het releasebeleid is duidelijk omschreven in de Service Level Agreement.	
Uitzonderingen	Niet van toepassing	

Versie 2.0

Titel Niet-Productie omgevingen (NPO)

Principe **Voor alle bronsystemen is er naast de productie-omgeving minimaal 1 niet-productie omgeving beschikbaar voor ontwikkel-, test- en trainingsdoeleinden beschikbaar.**

Rationale In onze beheer en ontwikkelprocessen is een extra omgeving noodzakelijk om op een beheerste en gecontroleerde manier nieuwe releases, interfaces, rapportages, etc te ontwerpen, te testen en vrij te geven. Bij voorkeur 2 omgevingen, minimaal 1.

Implicaties

1. Niet-Productie-omgevingen (NPO) staan niet op zichzelf maar maken deel uit van een integrale NP-informatievoorziening en voldoen op dezelfde manier aan de informatie-architectuurprincipes als de productieomgeving.
2. Het is mogelijk om een kopie te maken van de P-omgeving en deze in te lezen in één van de NP-omgevingen.
3. Het is mogelijk om een back-up te maken van een NP-omgeving en deze op een later moment terug te zetten zonder dat hier kosten aan verbonden zijn. Dit terugzetten mag niet meer dan een dag duren.
4. In NP-omgevingen worden geen productiedata beheerd. NP-omgevingen worden daarom geanonimiseerd op een manier dat een keten in de NP-omgeving blijft werken.

Uitzonderingen Testomgevingen, die voor het testen afhankelijk zijn van bestaande persoonsgegevens, worden uitgezonderd van het anonimiseren. De toegang tot die omgeving is beperkt tot ontwikkelaars, functioneel beheerders en testers, die bij die applicatie betrokken zijn. De reden waarom die betreffende testomgeving niet geanonimiseerd is, is in het beheerdocument vastgelegd.

Versie 2.0

Titel Service Level Agreement

Principe **Rechten en plichten van de leverancier met betrekking tot support, netwerkbelasting, point-in-time-recovery en performance door de leverancier zijn vóór in productiename vastgelegd in een met KW1C overeengekomen SLA.**

Rationale Het goed functioneren van een systeem is afhankelijk van een goede support van de leverancier.

Implicaties

1. Voor elk systeem en koppeling dient een overeengekomen SLA-document te bestaan. Daarin worden beheer- en performanceafspraken vastgelegd.
2. Leverancier neemt maatregelen dat de in de SLA gemaakte afspraken over uptime, beheersbaarheid en support worden geleverd.
3. Leveranciers nemen maatregelen zodat de in de SLA gemaakte afspraken zoals redundantie, netwerkbelasting worden geborgd.
4. Het SLA-document valt onder de verantwoordelijkheid van de systeem- of koppelingseigenaar.

Uitzonderingen Niet van toepassing

Versie 2.0

Titel Migratie van gegevens

Principe **Gegevens in een applicatie zijn bij het vervangen van een applicatie te migreren van de te vervangen naar de nieuwe applicatie.**

Rationale Indien gegevens in een te vervangen systeem nog een doel dienen omdat het gaat om actuele productiegegevens dan wel om gegevens die om redenen van analyses nog beschikbaar moeten zijn, moeten meegenomen kunnen worden naar een nieuw systeem.

Implicaties

1. Applicaties beschikken standaard over exportmogelijkheden van alle relevante productiegegevens.
2. Applicaties beschikken standaard over importmogelijkheden van relevante productiegegevens.

Uitzonderingen Niet van toepassing

Principe nummer	3.14	(12)
-----------------	------	------

Versie	2.0
--------	-----

Titel	Point-in-time-recovery
-------	------------------------

Principe	Leveranciers van bedrijf kritische bronsystemen zijn in staat om, in geval van calamiteiten, een herstel uit te voeren op de data tot op het tijdstip van de calamiteit.
----------	---

Rationale	De bedrijfsvoering mag minimale last hebben van calamiteiten in de bronsystemen of, in geval van in-the-cloud, van de omgeving waarin de bronsystemen zijn geplaatst. Gegevensverlies wordt tot een minimum beperkt.
-----------	--

Implicaties	Een point-in-time-recovery wordt beschreven in een Service Level Agreement
-------------	--

Uitzonderingen	Niet van toepassing
----------------	---------------------

Principe nummer	3.15	(7)
-----------------	------	-----

Versie	2.0
--------	-----

Titel	Microsoftplatform
-------	-------------------

Principe	Het KW1C gebruikt het Microsoftplatform als basis voor de informatievoorziening.
----------	---

Rationale	Het KW1C wil waar mogelijk standaardiseren. Applicaties moeten kunnen aansluiten bij die standaard.
-----------	---

Implicaties	Software van derden kan overweg met Microsoft producten en het Microsoftplatform waaronder: <ul style="list-style-type: none">• Microsoft Windows Server• Microsoft Windows• Microsoft SQL• Microsoft Azure• Microsoft Office
-------------	---

Uitzonderingen	Niet van toepassing
----------------	---------------------

Versie 3.0

Titel Identity & Access Management (IAM)

Principe **Toegang en autorisatie wordt gefaciliteerd door de IAM-voorziening van het KW1C.**

Rationale

Het KW1C wil studenten, medewerkers en andere betrokkenen bij de KW1C-community een veilige omgeving bieden waarin de privacy van iedereen wordt gewaarborgd. Voor een goede beveiliging van de informatievoorziening, devices, infrastructuur en locaties is het nodig dat identiteiten en rolgedreven autorisaties vanuit één centrale Identity & Access Management voorziening worden beheerd en gefaciliteerd.

Implicaties

1. Wijzigingen van identiteiten en autorisaties worden near real-time verwerkt, zodat de betrouwbaarheid van de toegangsfaciliteit is gegarandeerd.
2. Toegang tot de informatievoorziening gebeurt op basis van het need-to-know beginsel zoals vastgelegd in het KW1C-autorisatiebeleid.
3. Autorisaties tot KW1C systemen en gegevens worden (bij voorkeur) op basis van attributen/claims in een federatief bericht/token gefaciliteerd.
4. KW1C identiteiten verkrijgen via moderne authenticatie toegang tot de verschillende systemen in het KW1C applicatielandschap. (zie 3.7 Moderne Authenticatie)
5. Identiteiten die niet zijn oorsprong vinden bij KW1C en wel toegang tot de verschillende systemen in het KW1C applicatielandschap nodig hebben, verkrijgen toegang uitsluitend middels moderne authenticatie op basis van een contract.
6. Het bewaren van identiteiten en loggingsgegevens gebeurt niet langer dan is vastgesteld in het autorisatiebeleid van het KW1C."

Uitzonderingen Niet van toepassing

Versie 3.0

Titel Het KW1C integratieplatform

Principe **Integratie tussen bron- en doelsystemen gebeurt via het KW1C Integratieplatform.**

Rationale KW1C wil controle op de uitwisseling van gegevens tussen bron- en afnemende systemen. Gegevens uit bronsystemen worden daarom gerepliceerd naar het integratieplatform en van daaruit, eventueel voorzien van aanvullende metadata en logica, beschikbaar gesteld aan afnemende systemen.

Implicaties

1. Interfaces tussen twee applicaties verlopen niet rechtstreeks en daarmee altijd via het integratieplatform.
2. Leveranciers van afnemende systemen zorgen ervoor dat de systemen gegevens kunnen ontvangen vanuit het KW1C integratieplatform.
3. Leveranciers van toeleverende systemen zorgen ervoor dat de systemen gegevens kunnen leveren aan het KW1C integratieplatform.

Uitzonderingen Een directe koppeling tussen applicaties is toegestaan als:

1. het een formele koppeling betreft tussen een KW1C kernsysteem en een formele externe organisatie (DUO, Belastingdienst, SBB, UWV, ...);
2. KW1C heeft vastgesteld dat de uit te wisselen gegevens tussen bron- en afnemend systeem
 - a. (in de voor de koppeling vereiste vorm of samenstelling) uniek zijn voor de desbetreffende koppeling;
 - én
 - b. die gegevens (in die vorm of samenstelling) niet nodig zijn in het integratieplatform voor andere doeleinden;

Principe nummer	4.3	(18)
Versie	3.0	
Titel	Replicatie	
Principe	Replicatie (als volledige, transformatievrije, unidirectionele datasynchronisatie van brondatabase naar ODS) wordt gerealiseerd als standaard out-of-the-box databasereplicatie of als push-pull, in deze volgorde van voorkeur.	
Rationale	<p>Standaard out-of-the-box database replicatie is betrouwbaar, snel op te zetten en vergt qua onderhoud een minimale inspanning. Bovendien is de latency minimaal.</p> <p>Push-pull is maatwerk en vergt dus een ontwikkelinspanning. Tevens is er sprake van datalateny (die lineair stijgt met de frequentie van de pull-activiteiten).</p>	
Implicaties	<p>1. De leverancier van bronsysteem moet replicatie naar SQL-Server ondersteunen.</p> <p>of</p> <p>2. Leverancier van bronsysteem moet services bieden waarmee gegevens kunnen worden opgevraagd en een event-engine hebben waarmee wijzigingsberichten kunnen worden verstuurd.</p>	
Uitzonderingen	Niet van toepassing	

Principe nummer	4.5	(40)
Versie	3.0	
Titel	KW1C API's	
Principe	KW1C-API's worden via Azure API Management gepubliceerd.	
Rationale	<p>KW1C-API's worden via Azure API Management gepubliceerd ten behoeve van performance en beveiliging.</p>	
Implicaties	<p>1. Er worden autonome API's in de cloud aangeboden.</p> <p>2. API's worden beveiligd op basis van marktconforme en open beveiligingsstandaarden.</p> <ul style="list-style-type: none"> • OAuth2 en Open ID Connect <p>3. API-functionaliteit voldoet aan de volgende punten:</p> <ul style="list-style-type: none"> • De API is vindbaar, begrijpelijk en sterk getypeerd (strongly-typed). • De API is qua semantiek goed gedocumenteerd en qua syntax goed beschreven conform WSDL- of swagger-standaard. • De beschrijving van de interfaces zijn door KW1C zowel functioneel als technisch goed gedocumenteerd. 	
Uitzonderingen	Niet van toepassing	

Principe nummer	4.6	(38)
Versie	1.0	
Titel	Batch interfaces	
Principe	Batch-interfaces worden ontwikkeld met het Kw1cSyncer-framework.	
Rationale	Oplossingen die gerealiseerd worden met het Kw1cSyncer-framework zijn gebaseerd op het .NET framework dat genoeg API's bevat om met nagenoeg alle denkbare omgevingen te kunnen connecten.	
Implicaties	In geval van een batch-interface: 1. biedt de leverancier van het bronsysteem een mogelijkheid om alle records van een bepaalde entiteit in de applicatie op te halen. 2. biedt de leverancier van het doelsysteem een mogelijkheid om alle records van een bepaalde entiteit in de applicatie in te lezen.	
Uitzonderingen	Niet van toepassing	

Principe nummer	4.7	(27)
Versie	3.0	
Titel	Push-pull systematiek	
Principe	Bij een wijziging in een gegeven in een bronsysteem levert het bronsysteem een push-bericht aan een KW1C-service endpoint, waarna asynchroon de bijbehorende gegevens worden opgevraagd via een service van het bronsysteem.	
Rationale	Als out-of-the-box databasereplicatie niet mogelijk is, is het push-pull mechanisme een aanvaardbaar alternatief om (near) realtime over de gegevens te kunnen beschikken in de ODS. Voor het ontvangen van push-berichten stellen wij een service REST-endpoint ter beschikking die gegevens opslaat in een berichtentabel. Asynchroon worden deze berichten verwerkt met een component die services aanroept.	
Implicaties	1. Voor het push-gedeelte wordt een afgeschermd en beveiligde service gebruikt die korte mutatie-berichten ontvangt en opslaat in een mutatietabel. 2. Voor het pull-gedeelte wordt een component ingezet die het bericht compleet maakt door een service van het bronsysteem aan te roepen om vervolgens de ontvangen data naar een Stored Procedure in het ODS van KW1C te sturen die de data (in XML- of JSON-formaat) verwerkt in de betreffende replicatie-tabel.	
Uitzonderingen	Niet van toepassing	

Versie 2.0

Titel Leveranciers API's

Principe **Leverancier levert een standaard koppelvlak van API's**

Rationale Leverancier levert een standaard koppelvlak voor halen en brengen van benodigde data op basis van REST of GraphQL.

Implicaties

1. Er wordt een standaard koppelvlak aangeboden voor het halen en brengen van benodigde of gevraagde data.
 - REST of GraphQL
2. API's worden beveiligd op basis van marktconforme en open beveiligingsstandaarden.
 - OAuth2 en Open ID Connect
3. API-functionaliteit voldoet aan de volgende punten:
 - De API is vindbaar, begrijpelijk en sterk getypeerd (strongly-typed).
 - De API is qua semantiek goed gedocumenteerd en qua syntax goed beschreven conform swagger-standaard.
 - De beschrijving van de interfaces wordt door leverancier zowel functioneel als technisch goed gedocumenteerd.

Uitzonderingen Niet van toepassing

Principe nummer	5.1	(22)
Versie	3.0	
Titel	Externe identiteiten	
Principe	Externe identiteiten krijgen op basis van contractuele afspraken toegang tot de KW1C-informatievoorziening middels moderne authenticatie.	
Rationale	Externe gebruikers moeten op basis van vertrouwde identiteiten toegang krijgen tot expliciete delen van de KW1C-informatievoorziening.	
Implicaties	Met externe partijen worden afspraken gemaakt rondom aansluitvoorwaarden, een DAP en een datacontract. Het vertrouwen is gebaseerd op 3 condities: 1 Aansluitvoorwaarden: de afspraak met de externe partij waartoe de identiteiten behoren 2 Dossier Afspraken Procedures (DAP): afspraken over de manier waarop de afspraken worden ingevuld. 3 Het datacontract: de syntax en semantiek van de uit te wisselen gegeven"	
Uitzonderingen	Niet van toepassing	

Principe nummer	5.3	(70)
Versie	2.0	
Titel	KW1C bepaalt de inrichting van omgevingen in eigen beheer	
Principe	Inrichting van de door KW1C beheerde (delen van) de omgeving wordt bepaald door KW1C.	
Rationale	Om grip te kunnen houden op de huidige en toekomstige eigen beheerde omgevingen is het noodzakelijk in controle te zijn over de randvoorwaarden waaraan onderdelen van die omgeving moeten voldoen.	
Implicaties	1. KW1C bepaalt welke actieve netwerkcomponenten er kunnen worden opgenomen in het KW1C netwerk, en hoe ondersteunende netwerkdiensten zoals DNS en DHCP worden vormgegeven. 2. KW1C bepaalt welke versies van en welke soorten operating systemen er worden ondersteund binnen de omgeving.	
Uitzonderingen	Niet van toepassing	

Principe nummer	5.4	(69)
Versie	2.0	
Titel	Security by design	
Principe	Inrichting van nieuwe systemen of uitbreiding van bestaande systemen is altijd gebaseerd op standaard maximale beveiling vanuit het ontwerp, waarbij toegang alleen verschaft wordt als dat noodzakelijk wordt geacht.	
Rationale	Beveiliging van toegang tot systemen en gegevens is altijd inzichtelijk en te verantwoorden; hiermee is een eventueel risico op of impact van beveiligingslekken direct inzichtelijk en daardoor beheerbaar.	
Implicaties	1. Bij standaard firewall-inrichting wordt verkeer standaard geblokkeerd en expliciet open gesteld op verzoek. 2. Gebruikers- en beheertoegang tot nieuwe toepassingen wordt standaard beperkt tot de doelgroep(en) waarvoor die toegang verantwoordbaar is. Overige gebruikers en beheerders krijgen standaard geen toegang.	
Uitzonderingen	Niet van toepassing	

Principe nummer	6.2	(47)
Versie	2.0	
Titel	Responsive webdesign	
Principe	Applicaties en publicaties maken gebruik van een responsive webdesign.	
Rationale	Voor veel gebruikers en met name studenten is een mobiel apparaat (telefoon, tablet) de eerste toegang tot informatie. Applicaties en publicaties van gegevens dienen daarom responsive te zijn zodat ze op alle devices weergegeven kunnen worden.	
Implicaties	Bij het vormgeven van applicaties en publicaties dient altijd rekening gehouden te worden met een presentatie op een mobiel apparaat. Dat betekent, dat de performance van de publicatie moet aansluiten bij mobiel gebruik en dat de hoeveelheid data altijd tot een minimum beperkt moet worden.	
Uitzonderingen	Indien de hoeveelheid data in een publicatie dusdanig groot is, dat de publicatie niet geschikt is voor een weergave op een mobiel apparaat kan van het principe afgeweken worden.	

Versie 2.0

Titel Authenticated submit

Principe **Email vanuit of in naam van het KW1C wordt verstuurd via authenticated submit middels het cloud emailplatform van KW1C.**

Rationale Het versturen van email via deze methodiek garandeert de hoogste veiligheidstandaard, logging van het communicatieverkeer en bescherming tegen identiteitsfraude.

Implicaties Applicaties, die mailberichten versturen, maken gebruik van het cloud emailplatform van KW1C.

Uitzonderingen Niet van toepassing
