

Integrale architectuurprincipes

Integrale architectuurprincipes

Versiebeheer

Status	Door	Datum
Concept 0.1	Dennis Leenman	16-04-2020
	Besproken in werkgroep 2	16-04-2020
0.2	Werkpakket ICT / IM	25-06-2020
0.5	Dennis Leenman	12-09-2020
0.7	Werkpakket ICT / IM	29-09-2020
0.8	Dennis Leenman en Harmen Lindeboom	30-09-2020
0.9	Dennis Leenman en Harmen Lindeboom	26-10-2020

Integrale architectuurprincipes

Inhoudsopgave

1	Inleiding	4
1.1	Doel van deze notitie.....	4
1.2	Doelgroep	4
1.3	Samenhang met andere beleidsdocumenten	4
1.4	Waarom een Technische- en Informatie-architectuur.....	4
1.5	Principes en uitgangspunten Technische- en Informatie-architectuur.....	5
1.6	Vervolg en verdere ontwikkeling	5
1.7	Burchtmetafoor	6
1.8	De informatievoorziening overschrijdt organisatiegrenzen.....	7
1.9	Stabiliteit van de ICT voorzieningen heeft een hoge prioriteit	7
2	Achtergrondinformatie	8
2.1	DYA	8
2.2	Framework	8
2.3	Proces	9
3	Architectuurprincipes.....	10
3.1	Informatie principes	10
3.1.1	Passende informatie beschikbaar stellen.....	10
3.1.2	Bescherming persoonsgegevens	10
3.1.3	Eén centrale informatievoorziening.....	11
3.1.4	Generieke functionaliteit kent één applicatie.....	12
3.1.5	Eenmalige registratie, meervoudig gebruik	12
3.1.6	Inzage gegevensmodel koppelvlakken	13
3.1.7	Proces, data- en applicatie eigenaren	13
3.1.8	Standaard software boven maatwerk.....	14
3.1.9	Plaats en tijd onafhankelijke toegang tot de informatievoorziening	15
3.1.10	SLA – Exit strategie	15
3.2	Technische principes	15
3.2.1	Niet-Productie omgevingen (NPO).....	15
3.2.2	Bewezen technologie	16
3.2.3	Identity en Authorisation Management (IAM).....	16
3.3	Na de fusie.....	18
3.3.1	Gegevenswoordenboek.....	18
	Bronnen.....	19

Integrale architectuurprincipes

1 Inleiding

1.1 Doel van deze notitie

Deze notitie heeft als doel de nieuwe organisatie te begeleiden met een basisset aan architectuurprincipes. De basisset bestaat enkel uit de noodzakelijk principes voor de uitwerking van te harmoniseren systemen. Een volledige set zal in een latere fase (na de fusie) ontwikkeld worden.

1.2 Doelgroep

Deze basisset geeft clusters en werkpakketten richting bij het ontwikkelen van harmonisatievoorstellen.

1.3 Samenhang met andere beleidsdocumenten

Het informatiebeleid hangt samen met een aantal andere beleidsdocumenten en vertoont hier op onderdelen overlap mee. De focus ligt hierbij op de beleidsdocumenten die een direct effect hebben op de informatievoorziening en de ondersteuning hiervan.

- Informatiebeveiliging en Privacy-beleidsplan (IBP)
De bescherming van de gegevens binnen informatievoorziening is apart uitgewerkt in het IBP-plan en wordt beheerd door de IBP-manager.
- Informatieplan
De beschrijving van de informatievoorziening, haar processen, benodigde rollen en structuren.

1.4 Waarom een Technische- en Informatie-architectuur

Citaverde, Helicon en Wellant (en de daaruit voortkomende nieuwe organisatie) willen leerlingen en studenten optimaal voorbereiden op het beroepsleven en op vervolgonderwijs. Om deze ambitie te kunnen realiseren is een goede informatievoorziening onontbeerlijk, om de volgende redenen:

- Een goede informatievoorziening ondersteunt goed onderwijs. Door goed inzicht te hebben in de voortgang van leerlingen/studenten, hun verzuim, hun specifieke wensen en kenmerken kan een goede begeleiding worden gerealiseerd en kan het onderwijs worden toegesneden op de persoonlijke behoeftes van de individuele leerling/student.
- Een goede informatievoorziening ondersteunt een goede besturing van de organisatie. Door up-to-date informatie uit primaire bronnen op een goede manier te ontsluiten kan op diverse niveaus in de organisatie beter worden gestuurd.
- Een goede informatievoorziening maakt een efficiënte bedrijfsvoering mogelijk. Door zaken als eenmalige invoer / meervoudig gebruik, beschikbaarheid van correcte en up-to-date informatie en procesondersteuning met actuele applicaties kan een grote efficiencyverbetering in de bedrijfsvoering worden gerealiseerd. Dit maakt middelen vrij voor het primaire proces: het onderwijs;

Op al deze dimensies kan de informatievoorziening bijdragen aan substantiële verbeteringen. Om dit te realiseren is het echter nodig dat de informatievoorziening een logisch geheel wordt, dat het een gestructureerd systeem wordt waarbij de verschillende delen op elkaar aansluiten, elkaar aanvullen, met zo min mogelijk overlap. Een systeem onder architectuur.

Integrale architectuurprincipes

Informatiearchitectuur is hetzelfde als een bouw architectuur. Het biedt een ontwerp voor hoe het IT landschap er uit moet komen te zien. Kort gezegd is architectuur een manier om inzicht te krijgen en structuur aan te brengen in de informatievoorziening en ICT binnen een organisatie, en een manier om die te kunnen besturen.

Uiteindelijk gaat het erom te begrijpen waarom de informatievoorziening is opgebouwd zoals ze is opgebouwd, te beschrijven hoe de verschillende onderdelen zijn opgebouwd en met elkaar samenhangen, en te besturen hoe dat zich in de tijd gezien ontwikkelt.¹

Werken met architectuurprincipes betekent dat we gezamenlijke uitgangspunten en semantiek gebruiken die helpt bij besluitvorming zoals bij aanbestedingen en wijzigingen.

Zo'n samenhangend systeem biedt allerlei mogelijkheden voor de organisatie. Maar het vereist ook discipline, het besef dat niet alles altijd mogelijk is. Vooral bij bedrijfsvoeringssystemen is standaardisatie en het 'werken met architectuurprincipes' en processen cruciaal.

Deze architectuurprincipes leggen de kaders vast voor de harmonisatieprojecten die op ons af gaan komen.

1.5 Principes en uitgangspunten Technische- en Informatie-architectuur

Er zijn op diverse niveaus architecturen die een verschillende rol hebben. In de vakliteratuur wordt gesproken over Enterprise Architectuur, Business Architectuur, Informatie Architectuur, Applicatie Architectuur en Technische Architectuur.

Deze notitie beschrijft de architectuurprincipes van de technische- en informatie(/applicatie)-architectuur, die in dit kader gezamenlijk worden beschouwd. Deze architectuurprincipe stimuleren de samenhang in de manier waarop informatie wordt vastgelegd, uitgewisseld en gebruikt. In deze notitie worden de architectuurprincipes beschreven op inhoud, de motivatie, de implicaties en de borging.

1.6 Vervolg en verdere ontwikkeling

Een vervolgstap is om de diverse architectuurprincipes te operationaliseren: in hoeverre de huidige situaties afwijken van dit principe, en wat er nodig is om dit principe te realiseren in de nieuwe situatie.

In eerste instantie zullen de architectuurprincipes worden toegepast bij grootschalige wijzigingen van de informatievoorziening, zoals de het harmoniseren van het applicatielandschap, de vervanging van een bestaande applicatie of het introduceren van een nieuwe applicatie. In de besluitvorming wordt dan getoetst of de aanpassingen in lijn met de principes zijn.

Als de principes steeds verder worden betrokken, zullen deze ook worden betrokken op kleinere wijzigingen.

De architectuurprincipes worden getoetst in de praktijk en bijgesteld waar dit nodig blijkt. Informatiemanagement zal hier samen met functioneel beheer de regie op voeren.

¹ Twynstra Gudde kennisbank, ICT architectuur (<https://www.twynstraguddekennisbank.nl/node/1403>)

Integrale architectuurprincipes

De architectuurprincipes worden verder ontwikkeld en uitgebreid als hier aanleiding voor is. De uitbreiding is onderhevig aan besluitvorming. Uitbreidingen en (grote) aanpassingen worden vastgesteld door het College van Bestuur of een gedelegeerd gremium.

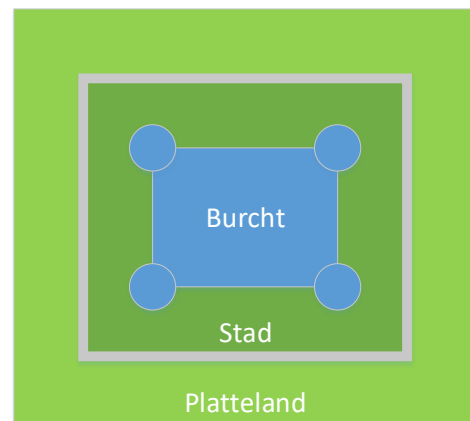
1.7 Burchtmetafoor

In het spreken over de informatievoorziening maken we gebruik van de “burchtmetafoor”. Deze metafoor verwijst naar de middeleeuwse inrichting van het landschap en gebruikt de bijbehorende termen om op hoofdlijnen te associëren of analogieën te introduceren.

Deze metafoor deelt het applicatielandschap op in drie delen, ook wel gebieden:

1. De Burcht – kernapplicaties

De burcht is de plek in het applicatielandschap waar het draait om stabiliteit en continuïteit. In de burcht treft je de kernapplicaties van de organisatie, voor zover het de registratie van gegevens betreft. Deze worden centraal beheerd, centraal aangestuurd en kennen strikte voorwaarden voor gebruik. Dat geldt ook voor de verbindingen naar de burchtapplicaties. De financiële administratie of een studenteninformatiesysteem zijn hier een goed voorbeeld van. De beweegruimte voor de individuele gebruiker is hier heel beperkt. Er wordt van de gebruiker verwacht dat deze zich conformeert aan het voorgeschreven gebruik.



2. De (open) Stad – generieke applicaties

In de stad treffen we de generieke applicaties die door meerdere onderdelen van de organisatie worden gebruikt. Deze applicaties worden meestal centraal beheerd en soms centraal aangestuurd. Een locatie heeft de keuze om hier gebruik van te maken, maar dat hoeft niet. Denk bijvoorbeeld aan Learnbeat, dat op een aantal locaties wordt gebruikt, maar niet organisatie breed.

3. Het platteland – vrije applicaties

Het platteland vormt het deel waar duizend bloemen bloeien, maar wel op eigen gelegenheid en kracht. Er is geen centrale ondersteuning. De gebruiker is zelf verantwoordelijk voor het gebruik en de ondersteuning van de door hem gekozen applicaties. Denk bijvoorbeeld aan een brainstorm tool op het web of het gebruik van YouTube.

Binnen de organisatie maken we op hoofdlijnen al gebruik van deze indeling, maar dit heeft aanscherping. In de praktijk praten we niet zo over onze applicaties en het is beperkt terug te zien in de besluitvorming en beleid. In de kern is het beheer van de burcht applicaties centraal belegd. De meer generieke (stad) applicaties vaak wel, maar niet altijd. De vrije applicaties (bijvoorbeeld onderwijs apps) vallen over het algemeen niet onder centraal beheer.

Integrale architectuurprincipes

Het is de bedoeling de burchtmetafoor structureler in te zetten in definities van taken en verantwoordelijkheden rondom applicaties en processen. Per deel wordt de “discipline” van dat deel vastgesteld en opgenomen in het beleid voor die applicaties of processen. Daarnaast wordt actief bewaakt of applicaties en processen in het juiste deel zitten en bij een transitie van het ene deel naar het andere deel wordt het beleid aangepast.

De architectuurprincipes zullen altijd met een “pas toe of leg uit”-beginsel worden toegepast. Echter, in de verschillende gebieden zal verschillend worden omgegaan hoe dit wordt beoordeeld. Op het platteland is veel meer ruimte voor het “leg uit” gedeelte, dan in de burcht.

1.8 De informatievoorziening overschrijdt organisatiegrenzen

We realiseren ons als geen ander dat onderwijs organisatiegrenzen overschrijdt. Naast ouderbetrokkenheid en BPV zullen studenten (en medewerkers) in toenemende mate gebruik kunnen maken van onderwijs dat buiten de instelling wordt verzorgd door andere instellingen via online kanalen. Als organisatie zullen we externe betrokkenen passende faciliteiten om informatie uit te wisselen moeten bieden met de interne informatievoorziening. De toegang tot onze informatie door derden vergt een slim (beheerarm) authenticatie- en autorisatiesysteem waarbij geborgd wordt dat persoonlijke informatie nooit bij onbevoegden terecht kan komen. De architectuurprincipes hebben deze randvoorwaarden in zich.

1.9 Stabiliteit van de ICT voorzieningen heeft een hoge prioriteit

Het onderwijs is zo afhankelijk geworden van de ICT voorzieningen, dat de impact van een verstoring zeer groot is. Als deze basis op orde is, is er ruimte voor verdere ontwikkelingen. Het is essentieel dat de ICT voorzieningen stabiel zijn. Dit is de basis voor iedere discussie of innovatie.

Dat stabiliteit betekent dat je concessies moet doen ten aanzien van innovaties mag duidelijk zijn. Nieuwe technieken, zeker als ze nog niet zijn uitontwikkeld, hebben risico's. Daarnaast is een onderwijsinstelling een complexe omgeving met veel verschillende belanghebbenden. De stabiliteit zal gewaarborgd moeten worden door zorgvuldige implementatie en inrichting van beheer. Het Team ICT is hierbij een noodzakelijke speler om dit te borgen.

Bij ontwerp keuzes is stabiliteit van de gehele keten altijd een zwaar wegende factor. Indien gekozen wordt voor lagere kosten of risico verhogende functionaliteiten, zullen de consequenties ten aanzien van het risico bij de besluitvorming geaccepteerd worden door de gebruikersorganisatie.

Dat wil uiteraard niet zeggen dat innovaties niet mogelijk zijn. Integendeel. Innovaties die de stabiliteit ondermijnen zullen met extra maatregelen omkleed moeten worden. Maar doordat er meteen naar de impact op de stabiliteit van de ICT voorzieningen gekeken wordt kan deze de innovatie versterken, waardoor de haalbaarheid vergroot wordt.

De inrichting van ons beheer wordt bepaald door het verkleinen van risico's en het verkorten van de oplostijd in geval van een calamiteit.

Integrale architectuurprincipes

2 Achtergrondinformatie

Het doel van deze notitie is om de clusters/werkgroepen een handvat te geven m.b.t. de informatievoorziening. Het is te veel om uit te weiden over het vertrekpunt van de architectuurprincipes, maar een korte beschrijving van de basis is nuttig om de beschreven principes in perspectief te zien.

2.1 DYA

Er is gekozen om op basis van het DYA (Dynamische Architectuur)² van Sogeti een begin te maken met het ophalen van principes die richting (gaan) geven aan de ICT-organisatie. DYA is een pragmatische benadering van architectuur met als uitgangspunt dat het primaire proces ondersteund wordt.

Principes realiseren de behoefte aan een inhoudelijk sturingsinstrument op een hanteerbaar abstractieniveau. Het architectuur framework wordt gevuld als een soort “ladekast” waarin alle principes een logische plaats krijgen.

2.2 Framework

De “ladekast” ziet er als volgt uit:

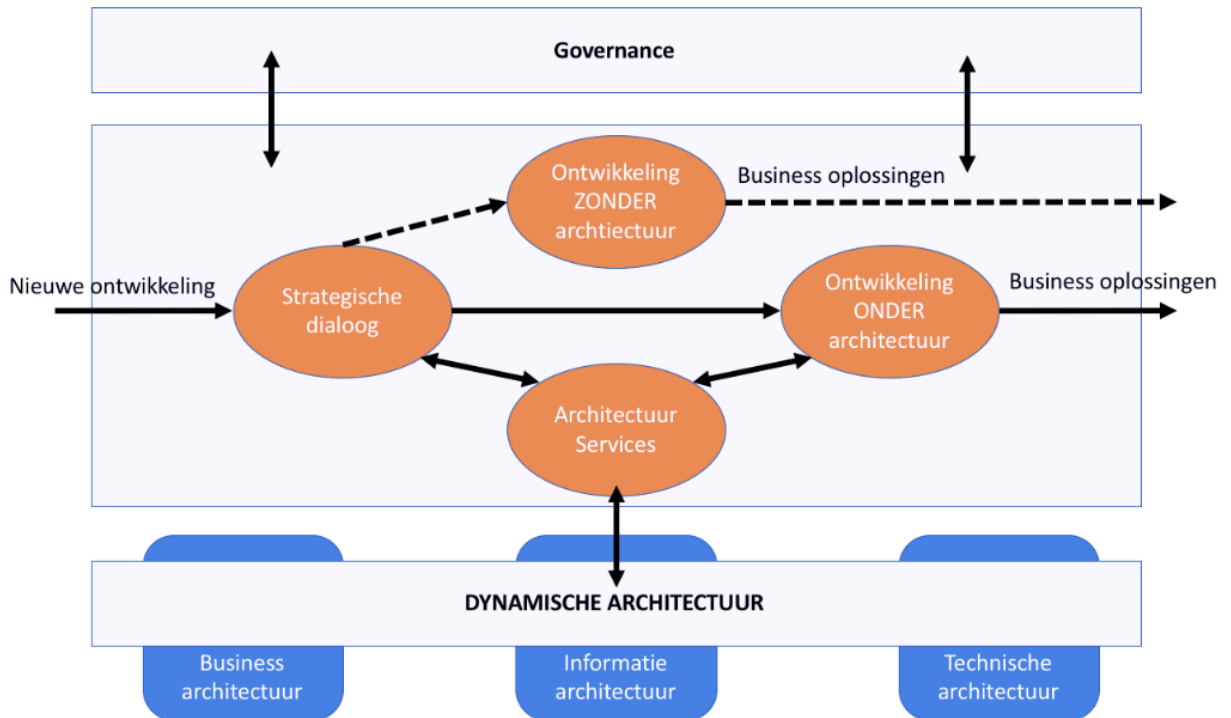
Business doelen									
	Business architectuur				Informatie architectuur		Technische architectuur		
	Kaders	Product / Dienst	Proces	Organisatie	Informatie	Applicatie	Middleware	Platform	Netwerk
Algemene Principes	Algemene principes								
Domein Principes	Business principes				Informatie Principes		Technische principes		
Modellen									

² <https://www.sogeti.nl/expertises/methodes/dya>

Integrale architectuurprincipes

2.3 Proces

Als proces ziet dat er als volgt uit:



Integrale architectuurprincipes

3 Architectuurprincipes

Deze notitie beperkt zich tot de principes, horende bij de technische en informatie architectuur.

3.1 Informatie principes

3.1.1 Passende informatie beschikbaar stellen

Principe	Medewerkers, leerlingen en studenten beschikken over alle informatie en functionaliteiten die ze nodig hebben om onderwijs te volgen of hun werk goed te kunnen uitvoeren, maar ook niet meer dan dat.
Toelichting	Om het werk te kunnen uitvoeren en te kunnen studeren moeten gebruikers benodigde informatie kunnen vinden, krijgen, bewerken, opslaan, doorgeven én opruimen, met alle bijbehorende functionaliteiten al naargelang de rol van de gebruiker. De informatievoorziening bevat functionaliteiten, die ondersteuning bieden aan gebruikers en er voor zorgen dat het werk en studie er makkelijker en leuker door worden. Dat een gebruiker niet meer informatie krijgt dan nodig dient twee doelen: op de eerste plaats krijgt de gebruiker geen overbodige informatie en op de tweede plaats beschermen we daarmee de privacy van iedereen waarvan informatie in de systemen is opgenomen. Dit is een continue dialoog tussen gebruiker, beheer en ontwikkeling over de passende informatievoorziening
Consequentie(s)	<ol style="list-style-type: none"> 1. De informatievoorziening is toegankelijk voor gebruikers op basis van een authenticatie en autorisatie, gekoppeld aan hun functie en rol in de organisatie. 2. Informatie en functionaliteiten worden zo veel mogelijk aangeboden op basis van de rol in de organisatie. 3. Standaardapplicaties moeten voor betrokken gebruikers binnen de daartoe gemaakte afspraken beschikbaar zijn. 4. De informatievoorziening maakt gebruik van actuele applicaties die rekening houden met en aangepast zijn aan de behoeften van het gebruik. 5.
Uitzondering	
Borging	

3.1.2 Bescherming persoonsgegevens

Principe	Met informatie en documenten wordt integer en vertrouwelijk gewerkt.
Toelichting	We beschouwen gegevens van leerlingen, studenten en medewerkers als kostbaarheden, die wij binnen de organisatie in bruikleen hebben.
Consequentie(s)	<ol style="list-style-type: none"> 1. De organisatie hanteert een informatiebeveiligings- en privacybeleid³ dat ten minste voldoet aan relevante wet- en regelgeving. Het opvragen, registreren, gebruiken, ontsluiten, bewaren en vernietigen van

³ Zie Informatiebeveiliging en Privacy-beleidsplan

Integrale architectuurprincipes

	<p>informatie en documenten gebeurt op basis van dit informatiebeveiligings- en privacybeleid.</p> <ol style="list-style-type: none"> 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-, data- en applicatie-eigenaren geclassificeerd volgens een BIV-classificatie⁴. 4. De organisatie hanteert een documentmanagementbeleid⁵. Op basis van dit beleid zijn de processen en systemen ten behoeve van het beheer van (digitale) documenten en het archief ingericht 5. Bedrijfs- en beveiligings-kritische systemen met het label "Hoog" op de onderdelen Integriteit of Vertrouwelijkheid, zijn aanvullend beschermd door middel van maatregelen, zoals Multifactor Authenticatie (MFA) en sterke versleuteling van gegevens in opslag en gegevens in transit. Systemen met het label "Hoog" op het onderdeel Betrouwbaarheid worden aanvullend beschermd door middel van redundantie in bijvoorbeeld elektra, opslagmogelijkheden, communicatielijnen of geografische scheiding.
Uitzondering	
Borging	IBP-plan

3.1.3 Eén centrale informatievoorziening

Principe	Beschikking over gegevens en functionaliteiten worden zoveel mogelijk vanuit één centrale informatievoorziening ⁶ beschikbaar gesteld.
Toelichting	Gebruikers ervaren zoveel mogelijk één informatievoorziening omdat gegevens en functionaliteiten in verschillende applicaties op een logische manier samenhangen en gebruikt kunnen worden. Daarbij hoeft een gebruiker niet steeds in te loggen in de bijbehorende bronapplicaties.
Consequentie(s)	<ol style="list-style-type: none"> 1. Een geïntegreerde informatievoorziening vergt een gedegen informatie-fundament met eenduidige definities, een helder gegevensmodel, benoemde data- en proceseigenaren en eenduidig beschreven gegevensbronnen. 2. Gegevens worden slechts éénmaal geregistreerd en onderhouden in een bronapplicatie en in andere applicaties hergebruikt, waar nodig. Afhankelijke applicaties betrekken de benodigde gegevens uit de bronapplicatie.

⁴ BIV-classificatie is een indeling die binnen de informatiebeveiliging wordt gehanteerd, waarbij de beschikbaarheid (continuïteit), de integriteit (betrouwbaarheid) en de vertrouwelijkheid (exclusiviteit) van informatie en systemen wordt aangegeven. Zie Informatiebeveiliging en Privacy-beleidsplan voor verdere toelichting

⁵ Nog in ontwikkeling

⁶ Informatievoorziening: het *geheel* van *mensen, middelen en maatregelen*, gericht op de *informatiebehoefte* van de organisatie. Het betreft dus niet alleen de gegevens en de applicaties, maar ook hoe we deze gebruiken, organiseren, onderhouden en vernieuwen.

Integrale architectuurprincipes

	<p>3. Waar een proces dat vereist, zijn de gegevens uit bronapplicaties real-time beschikbaar in afhankelijke applicaties.</p> <p>4. Een geïntegreerde informatievoorziening vergt een eenduidig autorisatieproces dat over alle functionaliteiten heen gaat.</p> <p>5. De ‘één informatievoorziening’-ervaring wordt nagestreefd door applicaties aan te passen aan de huisstijl.</p>
Uitzondering	
Borging	

3.1.4 Generieke functionaliteit kent één applicatie

Principe	Per generieke functionaliteit (in burcht en stad) is één applicatie actief.
Toelichting	Functionaliteit die hetzelfde doel hebben, bijvoorbeeld kernregistratie of onderwijsplanning, worden door één applicatie ondersteund. Elke applicatie vraagt beheercapaciteit, kennisonderhoud en licenties om deze goed in te kunnen zetten. Het efficiënt inzetten van deze middelen is gebaat bij het minimaliseren van het aantal applicaties. Daarnaast is de gelijkheid van gegevens en onderlinge verbanden binnen de functionaliteit beter te borgen in één applicatie.
Consequentie(s)	Functionele wensen worden eerst getoetst op het bestaande aanbod. Als de functionaliteit al beschikbaar is in de informatievoorziening, wordt deze eerst ingezet. Als toch een nieuwe applicatie wenselijk is voor bestaande functionaliteit, dan wordt de bestaande applicatie vervangen.
Uitzondering	
Borging	

3.1.5 Eenmalige registratie, meervoudig gebruik

Principe	Voor elk kerngegeven is één bronapplicatie aangewezen, waar de “waarheid” van dat gegeven wordt beheerd. Alle andere systemen die dezelfde gegevens gebruiken, leiden dit af van de bronapplicatie.
Toelichting	<p>Door een kerngegeven op één plek te beheren, kan de kwaliteit beter worden bewaakt. Andere systemen die het gegeven ook gebruiken hebben de verplichting dit gegeven actueel te houden vanuit die bron.</p> <p>Het vastleggen en onderhouden van een gegeven in één bronapplicatie is een voorwaarde om de betrouwbaarheid en integriteit van dat gegeven te kunnen garanderen.</p> <p>Het vastleggen van de definitie en eigenschappen van een gegeven in een centraal Informatiemodel garandeert dat informatievoorziening / -verstrekking op basis van dat gegeven eenduidig, betekenisvol en juist is en de betekenis overeenkomt met de definities uit de bedrijfsprocessen.</p>

Integrale architectuurprincipes

Consequentie(s)	<ol style="list-style-type: none"> 1. Van elk kerngegeven is bekend in welk proces en in welk bronsysteem het wordt geregistreerd. 2. Elk kerngegeven is opgenomen in het centrale informatiemodel. 3. Van elk kerngegeven is bekend wie de gegevenseigenaar is. Dit is in de regel de proceseigenaar van het proces waarin het gegeven wordt geregistreerd en onderhouden. 4. Bronsystemen moeten gegevens geautomatiseerd kunnen delen met andere systemen. Hier moet bij de inkoop en inzet van deze systemen rekening mee worden gehouden. 5. Kerngegevens kunnen in andere applicaties tot nieuwe informatie worden gewerkt, maar laten het oorspronkelijke gegeven intact. 6. Data en informatie in gebruikte bronapplicaties worden centraal beheerd.
Uitzondering	
Borging	Wijzigingen voor gegevens uitwisseling worden op dit principe uitgevoerd. Inventariseren voor welke gegevens dit op orde is en waar verbetering mogelijk is.

3.1.6 Inzage gegevensmodel koppelvlakken

Principe	Van alle bronsystemen is een gegevensmodel voor de koppelvlakken beschikbaar.
Toelichting	Voor het informatiemodel is het nodig dat kennis over de (meta) gegevens uit het bronsysteem en inzicht in het datamodel beschikbaar gesteld wordt.
Consequentie(s)	Leveranciers verstrekken een datamodel of een gegevensmodel van hun koppelvlakken, voorzien van adequate metadata en documentatie.
Uitzondering	
Borging	

3.1.7 Proces, data- en applicatie eigenaren

Principe	Elk proces heeft een proces-eigenaar. Elke applicatie heeft een applicatie-eigenaar. Gegevens die vanuit een proces worden verwerkt en in een applicatie worden geregistreerd hebben een data-eigenaar. Daar waar mogelijk is de proces-eigenaar ook eigenaar van de applicatie die het proces ondersteunt en eigenaar van de data die het proces verwerkt.
Toelichting	<p>Een proces-eigenaar is verantwoordelijk voor een goed verloop en daarmee de uitkomst van een proces. Dit omvat ook de verantwoordelijkheid voor de bescherming van de persoonsgegevens in het proces en de onderliggende systemen.</p> <p>Een applicatie-eigenaar is verantwoordelijk voor een goed functionerende applicatie en balanceert waar nodig de belangen van de betrokken processen en gebruikersgroepen.</p>

Integrale architectuurprincipes

	<p>De data-eigenaar is verantwoordelijk voor de juistheid en borging van de gegevens. Dit omvat ook de verantwoordelijkheid voor de bescherming van de persoonsgegevens naar andere systemen en buiten de processen.</p> <p>Het is mogelijk om deze verschillende eigenaarsrollen te combineren. Zie het informatieplan voor een nadere uitwerking.</p>
Consequentie(s)	<ol style="list-style-type: none"> 1. Een proces-eigenaar stelt de autorisaties vast van de gebruikers van de proces ondersteunende systemen. 2. Een proces-eigenaar stelt kwaliteitseisen op aan data, om te kunnen garanderen dat de applicatie het proces kan faciliteren. 3. Een applicatie-eigenaar stelt vast voor welk doel en in welke afnemende processen de geregistreerde data mogen worden gebruikt. 4. Een applicatie-eigenaar stelt vast welke functionaliteit zijn applicatie ondersteund en welke wijzigingenverzoeken worden uitgevoerd. 5. In voorkomende gevallen kan er een aparte proceseigenaar worden benoemd als een bepaald proces meerdere applicatie van verschillende applicatie-eigenaar gebruikt. In dat geval heeft de applicatie-eigenaar een serviceverlenende rol. 6. Een applicatie-eigenaar van een afnemende applicatie vraagt toestemming van de data-eigenaar van het leverende proces voor het gebruik van de data.
Uitzondering	
Borging	Uitgewerkt in het informatieplan

3.1.8 Standaard software boven maatwerk

Principe	Alle oplossingen worden gerealiseerd in standaard / off-the-shelf applicaties. Maatwerk wordt alleen als allerlaatste redmiddel ingezet. We hanteren "re-use, before buy, before make".
Toelichting	Het beheer en de verdere ontwikkeling van maatwerk-applicaties is arbeidsintensief en kostbaar. Maatwerk vormt daarmee een risico voor de informatievoorziening en dient zoveel mogelijk vermeden te worden.
Consequentie(s)	<ol style="list-style-type: none"> 1. We accepteren dat de mogelijkheden die de applicaties bieden voor een gedeelte onze processen vormgeven. 2. De software die de organisatie gebruikt wordt geleverd en onderhouden door leveranciers. De organisatie onderhoudt geen kennis voor het zelfstandig ontwikkelen en onderhouden van software op code niveau. 3. De organisatie onderhoudt geen infrastructuur voor het ontwikkelen van software.
Uitzondering	
Borging	

Integrale architectuurprincipes

3.1.9 Plaats en tijd onafhankelijke toegang tot de informatievoorziening

Principe	Gebruikers hebben toegang tot de informatievoorziening op elk moment, op elke plaats en vanaf elk gangbaar apparaat (anytime, anywhere, anyhow).
Toelichting	Gebruikers van de informatievoorziening werken deels of helemaal op eigen apparaten, die zij zelf meebrengen, binnen of buiten het college. De informatievoorziening moet daarom in een beveiligde omgeving ontsloten kunnen worden op die apparaten. Eigen devices maakt het risico op datalekken groter. Dit vergt maatregelen als devicemanagement en het opschonen van ingeleverde devices.
Consequentie(s)	<ol style="list-style-type: none"> 1. De organisatie stelt eisen aan het veilig gebruik van meegebrachte apparaten en extern gebruik van de informatievoorziening. Gebruikers conformeren zich impliciet aan de gestelde eisen. 2. Leerlingen, studenten en medewerkers 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. 5. Devices kunnen alleen toegang hebben tot niet-openbare informatie als deze onder het devicemanagement vallen.
Uitzondering	
Borging	

3.1.10 SLA – Exit strategie

Principe	We bepalen voordat een contract ingaat hoe de dienstverlening en beëindiging van het contract geregeld wordt.
Toelichting	Bij aanschaf van ICT producten moet worden afgesproken hoe bij continuïteit wordt geborgd en hoe de gegevens beschikbaar blijven als het contract wordt beëindigd. Door bij de aanschaf afspraken te maken hoe afscheid van elkaar genomen kan worden, zijn de verplichtingen over en weer vroegtijdig vastgelegd. Ook de dienstverlening tijdens de uitvoering van het contract wordt vooraf vastgelegd.
Consequentie(s)	1. Zonder afspraken rondom dienstverlening en beëindiging, bijvoorbeeld in een SLA/DAP/XLA, wordt er geen ICT contract ondertekend.
Uitzondering	ICT producten waarbij sprake is van een éénmalige transactie (alleen aanschaf, geen dienstverlening buiten wettelijke garantie, geen contract).
Borging	

3.2 Technische principes

3.2.1 Niet-Productie omgevingen (NPO)

Integrale architectuurprincipes

Principe	Voor alle bronsystemen zijn naast de productie-omgeving minimaal twee niet- productie omgevingen beschikbaar. Eén omgeving is geanonimiseerd beschikbaar.
Toelichting	In onze beheer- en ontwikkelprocessen zijn extra omgevingen noodzakelijk om op een beheerste en gecontroleerde manier nieuwe releases, interfaces, rapportages, etc. te ontwerpen, te testen en vrij te geven.
Consequentie(s)	<ol style="list-style-type: none"> 1. NP-omgevingen 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.
Uitzondering	Testomgevingen, die voor het testen afhankelijk zijn van bestaande persoonsgegevens, worden uitgezonderd van het anonimiseren. De toegang tot die omgeving is beperkt tot functioneel beheerders en testers, die bij die applicatie betrokken zijn. De reden waarom die betreffende testomgeving niet geanonimiseerd is, is in het beheerdocument vastgelegd.
Borging	

3.2.2 Bewezen technologie

Principe	We maken gebruik van leveranciers, oplossingen en technologieën met een bewezen staat van dienst (binnen het onderwijs).
Toelichting	Betrouwbaar, stabiel
Consequentie(s)	<ol style="list-style-type: none"> 1. We zijn hiermee trendvolger in het ontwikkelen van nieuwe oplossingen en technologieën. Door ook bij innovatie bewezen technologie te volgen kunnen we meteen naar de impact op de stabiliteit van de ICT voorzieningen kijken. Dat kan innovatie versterken, waardoor de haalbaarheid vergroot wordt.
Uitzondering	
Borging	

3.2.3 Identity en Authorisation Management (IAM)

Principe	Toegang en autorisatie (rechten toekennen) wordt gefaciliteerd door een centrale informatievoorziening
Toelichting	De organisatie wil leerlingen, studenten, medewerkers en andere betrokkenen bij de 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

Integrale architectuurprincipes

	<p>identiteiten vanuit één centrale Identity Authorisation Management voorziening worden beheerd en gefaciliteerd. Voor naadloze toegang tot applicaties en online diensten (Single Sign On) is een verbinding wenselijk, dit maakt een centrale IAM mogelijk.</p>
Consequentie(s)	<ol style="list-style-type: none"> 1. Wijzigingen van identiteiten 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. 3. Identiteiten verkrijgen (bij voorkeur) via federatieve koppelingen⁷ toegang tot de verschillende systemen in het applicatielandschap. 4. Identiteiten die niet zijn oorsprong vinden binnen de organisatie en wel toegang tot de verschillende systemen in het applicatielandschap nodig hebben, verkrijgen toegang uitsluitend via federatieve koppelingen op basis van een contract. 5. Het bewaren van identiteiten en loggingsgegevens gebeurt niet langer dan is vastgesteld in het autorisatiebeleid⁸
Uitzondering	
Borging	

⁷ Bij federatieve authenticatie wordt een vertrouwde partij gebruikt om authenticatie af te handelen voor toegang tot de eigen dienstverlening. Hierdoor kan eenvoudig en veilig worden ingelogd (geauthentiseerd) op eigen services door bijvoorbeeld klanten, leveranciers, partners waarmee wordt samengewerkt. - Organyze

⁸ Nog in ontwikkeling

Integrale architectuurprincipes

3.3 Na de fusie

Tijdens het harmoniseren kan er een begin gemaakt worden met dit principe. Het is echter nu nog te vroeg om een gegevenswoordenboek op te kunnen stellen. Nadat de fusie een feit is zal het gegevenswoordenboek wel met prioriteit opgepakt worden.

3.3.1 Gegevenswoordenboek

Principe	Gegevens zijn eenduidig beschreven in het gegevenswoordenboek
Toelichting	<p>Samenwerking en uitwisseling van gegevens is alleen goed mogelijk als die gegevens voor alle betrokkenen dezelfde betekenis hebben. Elk gegeven wordt daarom eenduidig beschreven in een gegevenswoordenboek.</p> <p>Een gegevenswoordenboek bevat een lijst van gegevenstypen (elementen) met een gegevensdefinitie die:</p> <ul style="list-style-type: none"> • omschrijft wat onder het gegeven moet worden verstaan; • op welke manier het gegeven wordt genoteerd (bv karakterset, datumnotatie, waardenlijsten); • aan welke bedrijfsregels het gegeven dient te voldoen.
Consequentie(s)	<ol style="list-style-type: none"> 1. Een gedefinieerd gegeven wordt als informatie-entiteit met de bijbehorende attributen en onderlinge relaties opgenomen in het informatiemodel. 2. De definitie van een gegeven kan onder vermelding van de reden afwijken van de definitie van dat gegeven in een bronsysteem. In die gevallen geldt voor het gebruik van het gegeven de organisatie-definitie. 3. Het vervangen van een bronsysteem leidt niet tot aanpassingen in een definitie. 4. Leveranciers voorzien de organisatie van eenduidige, volledige en actuele definities van gegevens in het bronsysteem, die via een API⁹ beschikbaar worden gesteld. 5. Elk gegeven in het gegevenswoordenboek heeft een eigenaar die verantwoordelijk is voor een eenduidige definitie, het juiste gebruik en het onderhoud van het gegeven. 6. Van elk gegeven is aangegeven in welke BIV-classificatie het gegeven valt: openbaar - intern - vertrouwelijk - geheim.
Uitzondering	
Borging	

⁹ API: een verzameling definities op basis waarvan een computerprogramma kan communiceren met een ander computerprogramma of onderdeel.

Integrale architectuurprincipes

Bronnen

Sogeti <https://www.sogeti.nl/expertises/methodes/dya>

Organyze <https://www.organyze.nl/artikelen/federatieve-authenticatie-lekentaal/>

Gesprekken

Jef van den Hurk (Koning Willem I)

Rob Goossens (Scamander)

Leden werkpakket

Tom Backx

Bert van Daalen

Arno Hartman

Theo Heijligers

Menno Hiemstra

Martijn van Hoorn

Victor de Kruyf

Dennis Leenman

Harmen Lindeboom

Luci Moorman

Alex Peeters

Jurriaan Phaff

Linda van der Sanden – Njiokiktjen

Rens van Uden