Architectuurprincipes Dienst ICT

Documenthistorie

Wijzigingsnummer:	1
Datum voltooid:	10-11-2020
Auteur:	Architectuur Board ICT / René van den Berg
Versie:	V1.0
Status:	Vastgesteld Architectuur Board
Bestandsnaam:	20201110 Architectuurprincipes Dienst ICT 1.0.docx

Revisies

Versie	Status	Datum	Wijzigingen
0.1	Concept	11-09-2018	Initiële Opzet
0.2	Concept	09-10-2018	Aanpassingen nav besprekingen met stakeholders
0.3	Concept	28-11-2018	Verwerking feedback MT
0.4	Concept	02-12-2018	Nieuwe feedback, met name FB NIET uitbesteden, RvdB
0.5	Concept	04-12-2018	Aanpassingen nav feedback
0.9	Concept	26-05-2019	RvdB, redactie
0.91	Concept	10-11-2019	RvdB, nav bespreking met SandraLAP en MarcZ
0.95	Review	22-10-2020	AB - Review & Tekstuele verbeteringen Architectuur Board Dienst ICT
1.0	Vastgesteld	10-11-2020	Vastgesteld binnen Architectuur Board Dienst ICT en aangeboden aan MT Dienst ICT

Bronnen

Naam	Datum	Toelichting
Triple A	01/08/2018	Triple A is het ICT architectuur framework voor het Middelbaar Beroeps Onderwijs in Nederland
HORA	01/08/2018	HORA is het ICT architectuur framework voor het Hoger Onderwijs in Nederland
Uitgangspunten Dienst ICT	15/09/2017	Eerdere versie van dit document
ICT VisiePlan 2018-2020	15/01/2018	Visie en ambitie van de Dienst ICT

BIV Classificatie

Beschikbaarheid

	Categorie	Toelichting
☞	Laag	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten
	Midden	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 48 uur brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten
	Hoog	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 4 uur brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten

Integriteit

	Categorie	Toelichting
	Laag	Het bedrijfsproces staat enkele integriteitsfouten toe
☞	Midden	Het bedrijfsproces staat zeer weinig integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk
	Hoog	Het bedrijfsproces staat geen integriteitsfouten toe

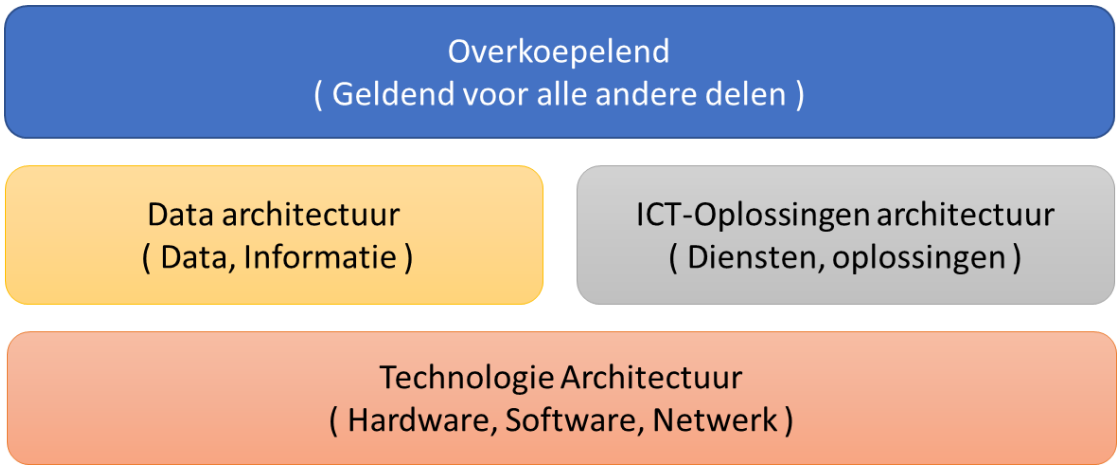
Vertrouwelijkheid

	Categorie	Toelichting
☞	Laag	Informatie die toegankelijk mag of moet zijn voor alle of grote groepen medewerkers of studenten. Vertrouwelijkheid is gering
	Midden	Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie is vertrouwelijk
	Hoog	Dit betreft zeer vertrouwelijke informatie, alleen bedoeld voor specifiek benoemde personen, waarbij onbedoeld bekend worden buiten deze groep grote schade kan toe brengen

Inhoudsopgave

1 Documentstructuur

Dit document gaat uit van de opdeling van de architectuur in 4 deelarchitecturen, te weten:



1. Overkoepelend: In de Overkoepelende deelarchitectuur komen de uitgangspunten ter sprake die van toepassing zijn op alle overige deelarchitecturen
2. Data: In de Data deelarchitectuur komen de uitgangspunten over data, informatie, dataclassificatie en beveiliging aan de orde
3. ICT-Oplossing: In de ICT-Oplossing deelarchitectuur worden de uitgangspunten en gehanteerde methodes rondom het bouwen van ICT-oplossingen besproken
4. Technologie: In de Technologie deelarchitectuur worden uitgangspunten voor het maken van technologische keuzes vastgelegd.

Aan iedere deelarchitectuur is in dit document een hoofdstuk gewijd aan de architectuurprincipes.

Na het goedkeuren van dit document zijn deze architectuurprincipes van toepassing op alle ontwerpen.

1 Inleiding

Dit document bevat de architectuurprincipes van de Dienst ICT van het ROCvA/ROCvF/VOvA. Deze principes dienen als richting en leidraad voor alle ontwerpen.

Dit document is tot stand gekomen door een analyse van de huidige situatie binnen de Dienst ICT, de architectuurprincipes vanuit SaMBO-ICT (Triple-A), SURF (HORA) en NORA en aangevuld met de kaders uit het ICT VisiePlan 2018-2020.

Ontwerpkeuzes dienen te worden verankerd in deze principes en mogen niet afwijken zonder een gedegen onderbouwing en acceptatie door het MT ICT. Hierbij dient in ogenschouw te worden genomen dat de architectuurprincipes zijn ontleend aan strategische, tactische en operationele doelen voor de organisatie als geheel. Afwijkingen doen mogelijk afbreuk aan deze doelen.

2 Begrippenlijst

Begrip	Definitie/Verklaring
AVG	Algemene Verordening Gegevensbescherming (in het Engels: General Data Protection Regulation)
Bedrijfsvoerings-applicatie	Applicaties die worden gebruikt bij de manier waarop de organisatie wordt bestuurd of beheerd
Beheerpartners	Ondersteunende, vaak externe partijen. Een leverancier welke beheertaken levert als dienst
BIV classificatie	Een BIV-classificatie of BIV-indeling 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. BIV is het acroniem voor Beschikbaarheid, Integriteit, Vertrouwelijkheid
Bronsysteem	Bronsystemen zijn systemen waar bepaalde gegevens initieel wordt geregistreerd en/of vanuit beschikbaar wordt gesteld. De bronsystemen bevatten broninformatie en/of deelinformatie over een digitaal gegeven die procesmatig naar andere systemen wordt getransporteerd
Cloud	Wereldwijd netwerk van servers, waarbij elke server zijn eigen functie heeft
Cloud model	Het Cloud model bestaat uit de lagen; SaaS, PaaS en IaaS
Dataregister	Een register van verwerkersactiviteiten, globale autorisatie en BIV classificaties
Dataverwerkende systemen	Dataverwerkende systemen vormen de ruggengraat van automatisering. Ze zijn bedoeld om door (letterlijk) automatisering schaalvergroting mogelijk te maken en kosten te besparen.
Dienst	Een transactie waarbij een niet-fysiek goed wordt geleverd
Generieke ICT	Applicaties waarbij functionaliteit via slechts één ICT-oplossing aan gebruikers wordt aangeboden
Het Nieuwe Werken	Een visie om werken effectiever, efficiënter maar ook plezieriger te maken voor zowel de organisatie als de gebruiker. Die visie wordt gerealiseerd door de gebruiker centraal te stellen en hem (binnen bepaalde grenzen) de ruimte en vrijheid te geven in het bepalen hoe, waar, wanneer, waarmee en met wie hij werkt
IaaS	Infrastructure as a Service Als je een IaaS afneemt, neem je de infrastructuur waar je diensten op draaien af van een externe partij. Infrastructuur bevat o.a. de componenten: • Compute • Netwerk • Opslag • Andere infrastructuur (back-up & security) De organisatie is zelf verantwoordelijk voor het configureren en onderhouden van de omgeving die op deze infrastructuur draait.
ICT-hardware	Dit betreft twee zaken: • Hardware t.b.v. eindgebruikers (devices) • Hardware t.b.v. ICT infrastructuur (servers, switches)
ICT-oplossing	Diensten die worden aangeboden aan de organisatie. Hieronder valt het ontwikkelen en/of beheren van systemen, netwerken, databases, applicaties en websites welke een dienst ondersteunen
Koppelvlak	Een interface die volgens een bepaalde standaard de uitwisseling van gegevens tussen dataverwerkende systemen verzorgt
Life Cycle Management	Een systematische aanpak van het beheer van de levenscyclus van een ICT-oplossing, vanaf het ontwerp en ontwikkeling tot de uiteindelijke totstandkoming inclusief het (eventuele) uit faseren
Modern	In de context van dit document verwijst modern naar recente of nieuwe applicaties, omgevingen of systemen
Modulair	Een systeem waarbij verschillende onderdelen uitwisselbaar zijn met andere onderdelen
Monolithisch	Wanneer iets een homogeen, moeilijk doordringbaar geheel vormt
Onderwijslogistieke applicatie	Systeem ter ondersteuning van het continue proces dat ervoor zorgt dat de leervraag van de studenten en het aanbod aan onderwijsproducten van de organisatie zo goed mogelijk op elkaar worden aangesloten
Op naam gesteld account	Een voor de organisatie unieke gebruikersnaam en wachtwoord welke gekoppeld is aan een natuurlijk persoon.

Organisatie-vertegenwoordigers	Specifieke gebruikers die namens andere gebruikers optreden om de belangen te behartigen
Paas	Platform as a Service De provider draagt zorg voor de inrichting van de infrastructuur. De organisatie is zelf verantwoordelijk voor de applicaties en hun bijbehorende inrichting. De PaaS-laag biedt een aantal diensten boven op de infrastructuur die het SaaS-aanbieders mogelijk maken hun toepassingen op een gestructureerde en geïntegreerde wijze aan te bieden. Voorbeelden van diensten in deze laag zijn toegangsbeheer, identiteitenbeheer, portaalfunctionaliteiten en integratiefaciliteiten.
SaaS	Software as a Service SaaS-providers leveren volledige en gebruiksklare softwarepakketten inclusief hosting. Deze diensten zijn volledig gericht op het gebruiksgemak van de eindgebruiker. De gebruikersorganisatie hoeft helemaal geen technische kennis te bezitten om gebruik te kunnen maken van deze oplossing. In veel gevallen zijn de SaaS-applicaties te gebruiken via een webbrowser op een computer.
Standaard platformen	Een platform is een (digitaal en smart) organisatiemodel dat gebruik maakt van een gedeelde basis van gestandaardiseerde organisatiebouwstenen: technologieën, infrastructuren, afspraken, competenties en standaarden of protocollen op basis waarvan meerdere toepassingen kunnen worden ontwikkeld. Een platform kan groeien tot een wereldwijde standaard.
TCO	Total Cost of Ownership, betreft de totale kosten die een product of dienst gedurende zijn hele gebruikscyclus met zich meebrengt
Verkregen hardware	Hardware die voor ICT personeel toegankelijk is, dan wel gehuurd, gekocht, geleased
Vraag en aanbod organisaties	Vraagsturing betekent het definiëren, afstemmen en bundelen van vragen vanuit organisatieprocessen (vraagkant). De inzet van technologische ontwikkelen(aanbodkant) zijn ondersteunend bij het specificeren van de vraag (wat)
WCAG	Web Content Accessibility Guidelines (WCAG) is een document dat is opgesteld en gepubliceerd door het World Wide Web Consortium (W3C) als onderdeel van hun Web Accessibility Initiative (WAI). De leidraad bestaat uit een verzameling richtlijnen voor de toegankelijkheid van web content, gericht op mensen met een beperking. Het volgen van deze richtlijnen maakt content ook toegankelijker voor webbrowsers en apparaten met beperkte functionaliteit zoals mobiele telefoons.

3 Principe Template

Template principe:

Naam	**<Naam van het principe>**
Principe	Het principe moet kort, duidelijk en precies de fundamentele ontwerpregel weergeven. De meeste principes voor het beheer van informatie lijken heel erg op elkaar tussen organisaties. Het is erg belangrijk dat de principes voor slechts één uitleg vatbaar zijn.
Rationale	De rationale geeft de zakelijke voordelen van het houden aan het principe aan. Beschrijf ook de relatie met andere principes en de bedoelde interpretatie en balans. Omschrijf situaties waarbij het ene principe zwaarder weegt dan het andere bij het nemen van beslissingen.
Implicaties	De implicaties geven op hoofdlijnen de eisen weer die gesteld worden aan de business en IT voor het uitvoeren van het principe, op de gebieden van resources, kosten, activiteiten en taken. Meestal is de huidige gang van zaken (systemen, standaarden) bij het invoeren van architectuur niet overeenkomstig met het principe, De impact op de business en de gevolgen van het houden aan het principe moeten duidelijk worden benoemd. De lezer moet eenvoudig antwoord kunnen krijgen op vragen als 'Hoe heeft dit betrekking op mij?'. Het is belangrijk om zaken niet te over-simplificeren, of te veroordelen. Implicaties kunnen reëel of potentieel zijn, volledig geanalyseerd of speculatief.

4 Overkoepelend

4.1 Architectuur is leidend

Naam	Architectuur is leidend
Principe	Architectuurprincipes zijn van toepassing op alle Diensten/ICT-oplossingen die door de Dienst ICT worden ondersteund en beheerd
Rationale	Een consistent en meetbaar kwaliteitsniveau kan worden geleverd aan de organisatie, wanneer de ICT-oplossingsontwerpen zich aan deze principes houden
Implicaties	1. Diensten/ICT-oplossingen worden getoetst aan de architectuurprincipes 2. Uitzonderingen op/afwijkingen van de architectuur kunnen alleen met onderbouwing en expliciete goedkeuring worden toegestaan 3. De architectuur is aan ontwikkeling en innovatie onderhevig. Ontwikkeling van de architectuur dient te worden geborgd om ervoor zorg te dragen dat de ICT-oplossingen van de Dienst ICT bijblijven bij de stand van de techniek en ICT-oplossingen 4. Verouderde architectuurprincipes worden structureel vervangen voor actuele varianten, via een jaarlijkse toetsing

4.2 Onderwijs Centraal

Naam	Onderwijs staat centraal
Principe	Bij alle initiatieven staat het Onderwijs centraal
Rationale	• Toenemende druk op kwaliteit en focus van onderwijs • Minder geld van de overheid • De student staat steeds meer centraal Dit stelt belangrijke vragen over waar prioriteiten liggen en waar tijd en geld aan wordt besteed. Het is belangrijk dat de primaire taken van onderwijsinstellingen daarbij bovenaan staan; dit is hun bestaansrecht Ondersteunende- en bedrijfsvoerings-processen zijn geen onderscheidende factor. Instellingen worden door de overheid gevraagd zich te profileren op hun onderscheidend vermogen op het gebied van onderwijs Zaken die niet direct bijdragen aan het primaire proces moeten goed worden gewogen
Implicaties	1. Alle investeringen worden beoordeeld op de mate waarin deze bijdragen aan onderwijs 2. Plannen en voorgenomen initiatieven worden afgeleid van de doelstellingen van de onderwijsinstelling en vervolgens beoordeeld en geprioriteerd 3. De inrichting van de ICT-oplossingen houdt rekening met het specifieke onderscheidend vermogen op het gebied van onderwijs, door hier specifieke functionaliteit voor aan te bieden 4. De ICT-oplossing die wordt aangeboden aan de organisatie is gebruiksvriendelijk, veilig en in lijn met technologische ontwikkelingen 5. Organisatie-vertegenwoordigers worden betrokken bij de inrichting van ICT-oplossingen, zodat deze optimaal aansluit bij hun belevingswereld en behoeften

4.3 Strategisch aankopen

Naam	Strategisch aankopen
Principe	Bij aankoopbeslissingen wordt gekozen voor een aankoop die het meest bijdraagt aan de architectuurprincipes
Rationale	Door de architectuurprincipes te wegen bij aankoopbeslissingen, worden beslissingen genomen die in lijn zijn met de strategische richting van Dienst ICT
Implicaties	1. Sector-breed aankopen verdient de voorkeur boven eigen aankoop 2. Er wordt ingekocht volgens het model 'Cloud first', waarbij SaaS oplossingen de voorkeur verdienen boven PaaS oplossingen, die op hun beurt de voorkeur verdienen boven IaaS oplossingen (SaaS>PaaS>IaaS) 3. Pas als een Cloud first oplossing niet mogelijk is, kan gekozen worden voor een oplossing waarbij de Dienst ICT, eigen ICT-oplossingen ontwikkeld op verkregen hardware

4.4 Leverancierskeuze

Naam	Beperkte leverancierskeuze
Principe	De leverancierskeuze voor ICT-oplossingen wordt beperkt
Rationale	Beperkte leverancierskeuze draagt bij aan minder complexe en beter geïntegreerde ICT-oplossingen
Implicaties	1. Er wordt een lijst bijgehouden van huidige leveranciers voor ICT-oplossingen 2. Bij huidige leveranciers en hun aangeboden ICT-oplossingen, wordt getoetst of hun oplossing voldoet

4.5 Organisatie Beheer

Naam	Organisatie beheer
Principe	Voor het organiseren van beheerswerkzaamheden wordt het 'Looijen' beheermodel gehanteerd gebruikt
Rationale	Dit beheermodel biedt een efficiënt en effectief managementsysteem voor het beheer van ICT-oplossingen. Dit draagt bij aan het principe *Prioriteit is Beschikbaarheid.* Het model van 'Looijen' is in onderwijsland een vaak gehanteerd model. Dit sluit aan op de manier waarop de huidige Dienst ICT is georganiseerd
Implicaties	1. Operationeel beheer is gesplitst in: Functioneel beheer, Applicatie beheer en Technisch beheer 2. Bij afspraken met interne organisatieonderdelen en/of andere organisaties hanteert de Dienst ICT dit model voor verantwoordelijkheden en definities

4.6 Functioneel beheer

Naam	Functioneel beheer
Principe	Functioneel beheer wordt zo veel mogelijk intern belegd.
Rationale	De complexiteit van ICT-oplossingen neemt toe, waardoor het voor de Dienst ICT toenemend moeilijk wordt om kennis van alle applicaties voldoende zelf te borgen met naleving van de principes *Onderwijs staat centraal* en *Prioriteit is Beschikbaarheid* Door het gebruik van standaard platformen voor applicaties is de uitdaging steeds minder het beschikbaar houden van deze applicaties, maar steeds meer het inzetten van deze applicaties om het Onderwijs centraal te stellen Aangezien functioneel beheer verantwoordelijk is voor de functies die mogelijk zijn binnen een applicatie, dient dit intern te worden uitgevoerd om zo de aansluiting van wensen van gebruikers en interne processen zo goed mogelijk aan te laten sluiten bij de inrichting van applicaties
Implicaties	1. Door gebruik te blijven maken van standaard platformen is de inkoop van applicaties eenvoudiger 2. Functioneel beheer krijgt ook kwaliteitsbewaking van de volledige keten (ICT-oplossing) in het takenpakket 3. Functioneel beheer wordt in toenemende mate de *linking pin* tussen vraag en aanbod organisaties

4.7 Applicatie beheer

Naam	Applicatie beheer
Principe	Applicatie beheer wordt waar mogelijk extern belegd
Rationale	De complexiteit van ICT-oplossingen neemt toe, waardoor het voor de Dienst ICT toenemend moeilijk wordt om kennis van alle applicaties voldoende zelf te borgen met naleving van de principes *Onderwijs staat centraal* en *Prioriteit is Beschikbaarheid* Door het gebruik van standaard platformen voor applicaties is de uitdaging steeds minder het beschikbaar houden van deze applicaties, maar steeds meer het inzetten van deze applicaties om het Onderwijs centraal te stellen
Implicaties	1. Interne competenties verschuiven van applicatiebeheer naar functioneel beheer, borging van applicatiebeheer verschuift naar de leverende partij

4.8 Technisch Beheer

Naam	Technisch beheer
Principe	Technisch beheer wordt waar mogelijk extern belegd
Rationale	De complexiteit van ICT-oplossingen neemt toe, waardoor het voor de Dienst ICT toenemend moeilijk wordt om kennis van alle componenten voldoende zelf te borgen met naleving van de principes *Onderwijs staat centraal* en *Prioriteit is Beschikbaarheid* Door het gebruik van standaard platformen voor applicaties is de uitdaging steeds minder het beschikbaar houden van deze standaard applicaties, maar steeds meer het inzetten van deze applicaties om het Onderwijs centraal te stellen
Implicaties	1. Interne competenties verschuiven van technisch beheer naar functioneel beheer, borging van technisch beheer verschuift naar de leverende partij

4.9 Modulair ontwerpen

Naam	Modulair ontwerpen
Principe	Ontwerpen zijn modulair, gelaagd en passend opgezet
Rationale	Modulaire en gelaagde ontwerpen staan toe dat losse modules een specifieke taak hebben, waarbij een module een duidelijk wat bijdraagt aan '*Prioriteit is Stabiliteit*' en passend aansluit op de vraag
Implicaties	1. De architectuur en ICT-oplossing worden gescheiden opgezet 2. Het onderbrengen van veel functionaliteit in 1 monolithisch component wordt voorkomen, zowel bij eigen ontworpen diensten als bij ingekochte diensten 3. Alleen functies van een product die nodig zijn worden geactiveerd, om onnodige complicaties te voorkomen

4.10 Compliancy

Naam	Compliancy
Principe	De organisatie, waar de Dienst ICT onder valt, voldoet aan Nederlandse wet- en regelgeving en aan de normen voor de publieke sector
Rationale	De organisatie is verplicht om aan de Nederlandse wet- en regelgeving te voldoen
Implicaties	1. De AVG verdient aandacht als nieuwe, toepasselijke wetgeving 2. Alle ICT-oplossingen zijn afdoende gelicentieerd voor hun beoogde doel 3. Voor alle organisaties binnen de publieke sector geldt een '*pas-toe-of-leg-uit*' verplichting. Dit betekent dat organisaties bij inkoop van ICT-systemen en -diensten boven € 50.000 moeten vragen naar de relevante open standaarden op de 'pas-toe-of-leg-uit' lijst van het Forum Standaardisatie[1]

[1] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/standaardisatie/open-standaarden/

5 Data Architectuur

ICT-oplossingen worden getoetst aan onderstaande principes, om te streven naar een zo goed en uniform mogelijk beeld op Data.

5.1 Archivering

Naam	**Archivering**
Principe	Archiefwaardige data wordt op een geschikte wijze bewaard
Rationale	Instellingen voeren een aantal openbaar gezag taken uit en hebben daardoor vanuit de archiefwet een verplichting bepaalde data blijvend te bewaren of te vernietigen na een bepaalde periode. Daarnaast hebben instellingen ook andere verplichtingen naar stakeholders en de maatschappij om bepaalde data te bewaren. Bovendien wordt vanuit de overheid sterker gestuurd op archivering van bewijsstukken van studenten. De archiveringsplicht is echter breder en heeft op veel data betrekking
Implicaties	1. Er is een organisatie-specifiek Document Structuur Plan (DSP) waarin alle soorten formele documenten, hun bewaartermijn en/of vernietigingstermijn zijn beschreven 2. Data wordt beheerd in de daarvoor aangewezen applicaties zodat zij op een later moment kunnen worden gereproduceerd 3. Applicaties zorgen ervoor dat de data die ze beheren op de juiste momenten worden bewaard of vernietigd 4. 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 5. Data die lang bewaard moet worden, blijft leesbaar doordat de daarvoor noodzakelijke apparatuur en programmatuur wordt bewaard of doordat deze wordt omgezet in een ander formaat

5.2 Kwaliteitsborging

Naam	**Kwaliteitsborging**
Principe	De kwaliteit van data wordt expliciet geborgd
Rationale	Data bepaalt in sterke mate de productie van organisaties; zonder data kunnen processen niet worden uitgevoerd. Voor onderwijsinstellingen geldt dit zo mogelijk nog sterker. Data is de basis van het onderwijs en zorgt ervoor dat informatie en kennis ontstaat en kan worden overgedragen op studenten, bedrijven en de maatschappij. Voor de bedrijfsvoering en ondersteunende processen is de kwaliteit van data essentieel; het is een bepalende factor voor de kwaliteit van de dienstverlening naar studenten, docenten en ondersteunend personeel. Management en bestuurders hebben kwalitatief hoogwaardige stuurinformatie nodig om de organisatie te kunnen besturen, bijvoorbeeld in het verhogen van de kwaliteit van het onderwijs. Kwaliteit van data kent vele dimensies zoals accuraat, compleet, actueel, beschikbaar, integer en vertrouwelijk. De kwaliteit van data moet vooral optimaal aansluiten bij het gebruik
Implicaties	1. Bij inrichting en veranderingen in de ICT-oplossing worden specifieke eisen gedefinieerd 2. Voor elke dataverzameling is een eigenaar aangewezen die verantwoordelijk is voor de kwaliteit van de data 3. Voor ieder relevant gegeven is er een eenduidige en gemeenschappelijke datadefinitie 4. Data wordt initieel op één plaats (bronsysteem) ingevoerd en beheerd

5.3 Risicoclassificatie data

Naam	**Risicoclassificatie data**
Principe	Data is beveiligd op basis van risicoclassificatie.
Rationale	Onderdeel van de kwaliteit van data zijn de aspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) die als kernonderdeel worden gezien van informatiebeveiliging. Ontwikkelingen als consumerisation, tijd- en plaats-onafhankelijk werken en cloud computing maken informatiebeveiliging ook een actueel onderwerp. Grenzen van organisaties vervagen en traditionele beveiligingsmaatregelen passen niet meer. Cybercriminaliteit kan zorgen voor ernstige ontregeling van de bedrijfsvoering. Het is daarom belangrijk de risico's expliciet te maken. Hierdoor kunnen de meest passende maatregelen worden genomen en worden overmatige- of ineffectieve maatregelen vermeden
Implicaties	1. Data zijn door de dataeigenaar voorzien van een BIV-classificatie die aangeeft wat het gewenste niveau van Beschikbaarheid, Integriteit en Vertrouwelijkheid is 2. Informatiebeveiligingsmaatregelen zijn gebaseerd op het Informatiebeveiligingsbeleid en de BIV-classificatie van de betrokken data 3. Maatregelen worden gebaseerd op een risico-analyse vanuit bedrijfsproces-perspectief 4. Informatiebeveiliging wordt integraal meegenomen bij het ontwerp en de inrichting van applicaties en infrastructuur 5. Naleving van regelgeving en informatiebeveiligingsmaatregelen is een verantwoordelijkheid van alle betrokkenen en wordt onder meer geborgd door periodieke interne en externe audits

5.4 Toegangsbeveiliging

Naam	Toegangsbeveiliging
Principe	Niemand mag ongeautoriseerd toegang hebben tot dataverwerkende systemen
Rationale	Omdat gebruik gemaakt wordt van een geïntegreerde informatievoorziening, bestaat een verhoogd risico op misbruik. Mensen die misbruik maken, moeten te allen tijde kunnen worden aangesproken, ook omdat de wetgever traceerbaarheid eist
Implicaties	1. Enkel data met een publiek karakter, zoals de publieke website, zijn anoniem / ongeautoriseerd beschikbaar 2. Het gebruik van elk op naam gestelde account valt te allen tijde onder verantwoordelijkheid van de gebruiker 3. De gebruiker is ervoor verantwoordelijk dat niemand het wachtwoord van zijn/haar op naam gestelde account kent 4. De gebruiker mag alleen zijn/haar op naam gestelde account(s) gebruiken 5. Niet op naam gestelde accounts zijn onderworpen aan een streng beleid (periodiek getoetst) en worden alleen toegestaan indien strikt noodzakelijk

5.5 Koppelingen

Naam	Beperkt aantal koppelingen
Principe	Koppelingen tussen systemen zijn beperkt tot alleen noodzakelijke data uitwisseling
Rationale	Door koppelingen te beperken tot alleen noodzakelijke data uitwisseling wordt geborgd dat er niet onbedoeld data buiten het zicht van de organisatie raakt. Bovendien biedt dit de mogelijkheid om het principe van één datamodel af te dwingen, samen met Toegangsbeveiliging. De organisatie is verantwoordelijk voor de vertrouwelijkheid van deze data en deze data dienen juist en proportioneel te worden uitgewisseld
Implicaties	1. Koppelingen tussen dataverwerkende systemen worden verzorgd door de Dienst ICT, of door hen aangewezen partijen 2. Iedere koppeling tussen dataverwerkende systemen heeft een ontwerp waarin minimaal de inhoud van dataset met BIV-waardering omschreven wordt, en maatregelen die zijn getroffen om de beschikbaarheid, integriteit en vertrouwelijkheid te borgen 3. Alle datauitwisseling vindt beveiligd plaats op basis van open- en gestandaardiseerde koppelvlakken

6 ICT-oplossing architectuur

6.1 Geïntegreerde informatievoorziening

Naam	Geïntegreerde informatievoorziening
Principe	Het is belangrijk dat gebruikers optimaal worden ondersteund in hun dagelijkse werk. Gebruikers willen direct toegang tot alle voor hen relevante informatie. Het raadplegen van de informatievoorziening mag geen drempels opwerpen.
Rationale	Het wegnemen van drempels bij toegang tot relevante informatie bij het dagelijkse werk leidt tot meer efficiënte processen, lagere kosten en een beter dienstverleningsniveau. Hiervoor is het belangrijk dat in elke processtap alle noodzakelijke informatie beschikbaar is. Gebruikers worden nog te vaak geconfronteerd met een versnipperde informatievoorziening doordat applicaties niet optimaal geïntegreerd zijn. Overigens moet worden voorkomen dat een te grote integratie kan leiden tot complexiteit in veranderingen binnen het applicatielandschap.
Implicaties	1. Een gepersonaliseerd portaal is het startpunt voor de gebruikers van de organisatie 2. Applicaties zijn geïntegreerd met andere applicaties die voor de gebruiker relevante gegevens of functionaliteit bevatten 3. Applicaties gebruiken gegevens uit de authentieke bron (bronsysteem) met vanuit het proces gewenste actualiteit 4. Applicaties bieden gestandaardiseerde koppelvlakken (services) op basis van open of de facto standaarden 5. Applicaties die zelf geen gestandaardiseerde koppelvlakken bieden worden geïntegreerd middels een eigen integratievoorziening conform een goed gedefinieerd gegevensmodel 6. Alleen de functionaliteit die aan een bepaalde processtap bijdraagt wordt vanuit een applicatie aangeboden

6.2 Organisatie overschrijdend leren en werken

Naam	Organisatie overschrijdend leren en werken
Principe	De inrichting van processen en systemen ondersteunt samenwerking op afstand en met derden
Rationale	Onder invloed van globalisering en digitalisering speelt samenwerking met derden een steeds grotere rol In het onderwijs zien we de instellingsgrenzen vervagen door het hybride leren (PPS) en de ontwikkeling van onlineonderwijs
Implicaties	1. Externen, personen niet werkzaam bij de organisatie, kunnen (na vaststelling van hun identiteit) eenvoudig toegelaten worden tot delen van de informatievoorziening 2. Binnen een identity management systeem worden alle identiteiten beheerd 3. Het identity management systeem is aangesloten op een (of meerdere) toegangsdiensten. Hierdoor kan de organisatie gecontroleerd aangeven met wie de gebruikers kunnen samenwerken met derden buiten de organisatie 4. Het identity management systeem heeft de mogelijkheid om identity gegevens uit geautoriseerde bronnen te benutten

6.3 Duurzame inrichting

Naam	Duurzame inrichting
Principe	Informatietechnologie wordt duurzaam ingericht en ingezet.
Rationale	De grondstoffen van de aarde zijn beperkt en kunnen opraken. Daarnaast kent de opnamecapaciteit van de atmosfeer en onze natuurlijke omgeving haar grenzen. We realiseren ons allemaal dat we de natuur moeten sparen en de opwarming van de aarde zoveel mogelijk moeten voorkomen. Voor publieke onderwijsinstellingen betekent duurzaamheid in ieder geval een verplichting om te voldoen aan landelijke doelstellingen en convenanten met de overheid. Het gebruik van ICT-oplossingen draagt voor een groot deel bij aan het energieverbruik van de organisatie.
Implicaties	1. Duurzaamheid is een vast onderwerp bij inkoop en inrichting. Er wordt gelet op de aspecten van de ~~energieverbruik~~ duurzaamheid van de ICT-oplossing 2. Bij de herinrichting van rekencentra wordt onderzocht in hoeverre uitbesteding of gemeenschappelijke rekencentra helpen bij het realiseren van een grotere mate van duurzaamheid in het algemeen en energie-efficiëntie in het bijzonder 3. Afgeschreven apparatuur wordt her-ingezet of duurzaam verwerkt (kringloop) 4. Apparatuur die langere tijd niet wordt gebruikt wordt automatisch stand-by geschakeld met als voorkeur uitgeschakeld 5. Data die niet meer gebruikt wordt of bewaard dient te blijven wordt verwijderd

6.4 Standaard applicaties

Naam	Standaard applicaties
Principe	Applicaties zijn waar mogelijk gestandaardiseerd.
Rationale	De organisatie richt de aandacht maximaal op onderwijs. Bedrijfsvoering, onderwijslogistiek en generieke ICT-oplossingen zijn een noodzakelijke randvoorwaarde, maar zeker geen onderscheidende factor voor de organisatie. Door gebruik te maken van standaard applicaties (onderhouden door de industrie) worden gestandaardiseerde hoofdprocessen ondersteund. De organisatie kiest voor één gemeenschappelijke applicatie. Extra investeringen en exploitatiekosten worden voorkomen en er kan geprofiteerd worden van schaalvoordelen. Het geld dat hierdoor vrijkomt kan worden geïnvesteerd in onderwijs. Standaardiseren daar waar de gebruiker geen hinder ondervindt, creëert ruimte voor flexibiliteit daar waar onderwijs centraal staat.
Implicaties	1. Er zijn organisatiebrede applicaties voor bedrijfsvoering, onderwijslogistiek en generieke ICT er zijn geen andere applicaties in gebruik die dezelfde functionaliteit bieden 2. organisatiebrede applicaties zijn bewezen in de praktijk en worden breed gebruikt binnen de sector 3. Wensen vanuit de organisatie voor applicatie specifieke uitbreidingen en aanpassingen worden sector breed getoetst. Maatwerk die enkel geldt voor de eigen organisatie wordt ontmoedigd 4. De standaard ingerichte processen behorend bij de applicatie worden overgenomen bij de inrichting van organisatiebrede processen

6.5 Prioriteit is Beschikbaarheid

Naam	Prioriteit is Beschikbaarheid
Principe	De beschikbaarheid van ICT-oplossingen heeft de hoogste prioriteit.
Rationale	Het onderwijs is dermate afhankelijk van ICT-oplossingen dat hierdoor de impact van een verstoring erg groot is. De mate van prioriteit is direct gekoppeld aan de 'B' uit de 'BIV' classificatie
Implicaties	1. Bij ontwerpkeuzes is de beschikbaarheid van de gehele keten altijd een zwaarwegende factor 2. Lagere kosten voor risico verhogende keuzes voor functionaliteiten zullen alleen worden gerealiseerd na acceptatie door de organisatie 3. Innovaties en ontwikkelingen die de stabiliteit mogelijk ondermijnen worden met extra maatregelen omkleed, bijvoorbeeld door het toepassen van een scheiding tussen Ontwikkel, Test, Acceptatie en Productieomgevingen 4. Het beheer richt zich op het verkleinen van risico's, het verkorten van oplostijden en structurele verbetering van geconstateerde defecten in ICT-oplossingen 5. De organisatie is leidend bij het vaststellen van de beschikbaarheidseisen van ICT-oplossingen

6.6 Gebruikte ICT-hardware

Naam	Gebruikte ICT-hardware
Principe	Er worden zakelijke edities van ICT-hardware aangeschaft, in plaats van consumentenversies
Rationale	Bij zakelijke edities van ICT-hardware zijn afspraken gemaakt tbv in voorraad houden van componenten, met een gegarandeerde levertijd, waardoor stabiliteit van dienstverlening beter kan worden geborgd. Daarnaast is afvoer van componenten geregeld
Implicaties	1. Consumentenversies van hardware worden niet aangeschaft ondanks het mogelijke investeringsvoordeel bij aanschaf 2. De marktuitvragen voor ICT-hardware moeten worden aangepast aan de behoeften vanuit de organisatie 3. ICT-hardware wordt conform Life Cycle Management periodiek procesmatig bijgehouden

7 Technische Architectuur

7.1 Elk moment, elke plaats, elk apparaat

Naam	Elk moment, elke plaats, elk apparaat
Principe	Geautoriseerde gebruikers hebben toegang tot applicaties op elk moment, op elke plaats en vanaf elk modern apparaat.
Rationale	Mensen willen steeds meer leren en werken op het tijdstip en de plaats waarop het hen het beste uitkomt. Dit is een kernonderdeel van Het Nieuwe Werken, waarbij voor verschillende werkzaamheden ook verschillende werkomgevingen worden gebruikt. Dat kan zijn overdag op kantoor, onderweg of 's avonds thuis Mensen willen zelf bepalen welke apparatuur en applicaties ze gebruiken. Mobiele telefoons, tablets en notebooks zijn gemeengoed geworden en mensen willen ze graag overal mee naar toe kunnen nemen en gebruiken (Bring Your Own Device) Veel applicaties zijn 'gratis' op Internet beschikbaar en sluiten mogelijk beter aan bij behoeften dan beheerde applicaties. Deze veranderingen in het gedrag en de behoeften van gebruikers moeten door de applicatie worden gefaciliteerd. Mits er voldaan blijft worden aan geldige wet- en regelgeving (bijvoorbeeld AVG) De applicatie dient ook beschikbaar te zijn voor gebruikers met een functiebeperking
Implicaties	1. Applicaties dienen zoveel mogelijk vanuit het SaaS model aangeboden te worden 2. Traditionele applicaties worden zo spoedig mogelijk aangepast naar dit model 3. Studenten en medewerkers kunnen hun eigen mobiele apparatuur (smartphone, tablet en notebook) meenemen naar de organisatie en daarmee toegang krijgen tot het applicatielandschap, zolang de apparatuur aan de aansluitvoorwaarden voldoet 4. De inrichting van het netwerk en de beveiliging gaan ervan uit dat het niet uitmaakt of gebruikers zich op het interne netwerk bevinden of op een externe locatie. Applicaties worden op een uniforme wijze benaderd 5. Applicaties die breed beschikbaar moeten zijn bieden ook een gebruikersinterface die specifiek is geoptimaliseerd voor weergave op een smartphone 6. Binnen de organisatie is een draadloos netwerk beschikbaar, met een vergelijkbare kwaliteit en capaciteit als het vaste netwerk. Het draadloze netwerk heeft voldoende capaciteit voor gelijktijdig gebruik van meerdere devices per gebruiker. Internet net als thuis 7. Er is bij het ontwerp en/of de selectie van applicaties specifiek rekening gehouden met gebruikers met een functiebeperking, in ieder geval door deze te toetsen aan de WCAG (wet-en regelgeving van toepassing op semi-overheidsorganisaties, sinds september 2020)

7.2 Samenwerkingsplatform

Naam	Samenwerkingsplatform
Principe	De organisatie werkt samen op een geselecteerd samenwerkingsplatform
Rationale	Door te kiezen voor één samenwerkingsplatform wordt bijgedragen aan de principes 'Elk moment, elke plaats, elk apparaat' en 'Informatiebeveiliging' principes, daarnaast is het principe 'Geïntegreerde informatievoorziening` goed te combineren
Implicaties	1. Andere samenwerkingsplatformen worden niet ondersteund en worden door de organisatie ontmoedigd 2. Bij gebruik van een ander samenwerkingsplatform, zijn gebruikers zelf verantwoordelijk voor alle functionaliteiten en naleving van regelgeving en informatiebeveiligingsmaatregelen 3. Gebruikers handelen conform de door de organisatie opgestelde ICT-gedragscode

7.3 Actueel

Naam	Actueel
Principe	ICT-oplossingen worden door middel van een proces actueel gehouden
Rationale	Actuele ICT-oplossingen dragen bij aan • acceptatie door gebruikers • het principe Prioriteit is Beschikbaarheid • veiligheid en gebruik
Implicaties	1. Voor iedere ICT-oplossing is een Life Cycle Management afspraak aanwezig 2. Het nakomen van Life Cycle Management afspraken maakt integraal onderdeel uit van de dienstverlening van Dienst ICT 3. Applicaties lopen in de regel maximaal 1 release achter (N-1) op de actuele versie 4. Software gebruikt op ICT hardware loopt in de regel maximaal 1 release achter (N-1) op de actuele versie

7.4 Netwerkfunctionaliteit

Naam	Netwerkfunctionaliteit
Principe	Het netwerk biedt snel en veilig transport naar internet
Rationale	In het kader van het principe 7.1 'Elk moment, elke plaats, elk apparaat' moeten alle applicaties, welke intern beschikbaar zijn, ook via het internet extern benaderbaar zijn De inrichting van het netwerk en de beveiliging ervan gaan ervan uit dat het niet uitmaakt of gebruikers zich op het interne netwerk bevinden of op een externe locatie
Implicaties	1. Het netwerk heeft een open en transparant karakter ten behoeve van alle gevalideerde gebruikers 2. Intern georganiseerde connectiviteit wordt afgebouwd. ICT-oplossingen worden via het internet ontsloten 3. Er is een uitgebreid draadloos netwerk beschikbaar, met een vergelijkbare kwaliteit en capaciteit als het vaste netwerk 4. Netwerkgebruik wordt geautomatiseerd bewaakt op misbruik

7.5 Werkplekken

Naam	Werkplekken (is een werkomgeving)
Principe	Werkplekken worden zo efficiënt mogelijk beheerd en aangeboden
Rationale	Vanaf elk apparaat is het mogelijk een werkplek te gebruiken. Volgens het principe 'Elk moment, elke plaats, elk apparaat' Door werkplekken logisch (apparaat onafhankelijk) aan te bieden is de inzet van een BYOD mogelijk. Hierdoor kunnen de fysieke werkplekken sterk gereduceerd worden
Implicaties	1. Een ICT-oplossing voor het logisch aanbieden van een werkplek dient beschikbaar te zijn. 2. Een actief beleid is vereist om het applicatie landschap over te zetten op een Cloud model, via de browser benaderbaar. 3. Door het loskoppelen van het fysieke apparaat van de werkplek, is het niet meer noodzakelijk een standaard ingerichte fysieke werkplek te blijven ondersteunen. Slechts minimumeisen hoeven te worden vastgesteld voor het BYOD. 4. Voor fysieke werkplekken m.b.t. examinering worden aanvullende eisen gesteld conform het geldende examenprotocol.

7.6 Service georiënteerd

Naam	Service georiënteerd ontwerp
Principe	Service-oriëntatie, service-oriented architecture (SOA), is een architectuurmodel, geen technologie op zich. Centraal bestaat een SOA-opgebouwd systeem uit servicecontracten. Hierbij is sprake van afnemers van ICT-oplossingen en leveranciers.
Rationale	Service georiënteerde architecturen zijn uitermate geschikt voor het modulair kunnen inzetten van toepassingen in SaaS en PaaS afnamemodellen
Implicaties	1. Een service is virtueel: de afnemer heeft geen weet van de implementatie van de dienst. De ICT-oplossing is onafhankelijk van de afnemer. Scheiding van verantwoordelijkheid is expliciet vastgesteld 2. Een service is gestandaardiseerd: er is slechts één implementatie aanwezig van een verantwoordelijkheid 3. Een service is modulair (vervangbaar) en compositioneerbaar. Standaard betekent echter niet direct flexibel. Flexibiliteit wordt bereikt door combineren (componeren) van standaarden tot een nieuwe standaard 4. Een service is abstract: generiek, niet afgestemd voor 1 specifieke afnemer, maar op een doelgroep van afnemers 5. Losgekoppeld: afnemer en leverancier zijn maximaal onafhankelijk van implementatie van beide. Elke service is daarom autonoom. Er bestaat geen directe link of relatie tussen verschillende services. Services zijn zich ook niet van elkaar bewust. 6. Eigenaarschap van ICT-oplossingen is geborgd 7. Lifecycle van ICT-oplossingen is geborgd

7.7 Schaalbaarheid

Naam	**Schaalbaar ontwerpen**
Principe	Nieuwe ontwerpen hebben een modulaire opzet, waarbij schaalbare aanpassingen eenvoudig te realiseren zijn
Rationale	Schaalbaar ontworpen ICT-oplossingen zorgen voor een goede aansluiting bij het principe 'Service georiënteerd ontwerp' en maakt aanpassing in capaciteit en beschikbaarheid mogelijk zonder architectuuraanpassingen
Implicaties	1. Nieuwe ontwerpen gaan uit van schaalbare modules 2. Bewaking vindt plaats op functie en schaalbaarheid, niet op capaciteit van individuele modules 3. Monitoring en capaciteitsbewaking van de gehele ICT-oplossing is ingeregeld 4. Bij selectie van een SaaS/PaaS/IAAS leverancier wordt schaalbaarheid in het ontwerp als criterium opgenomen 5. ICT-oplossingen kunnen snel op wijzigende omstandigheden worden geschaald. Traditionele over-dimensionering wordt hierdoor voorkomen