Clouddiensten

Beleidskader

Dienst ICT - Amsterdam UMC

Van: Tom Driessen, Peter Baltus & Valesca van Zwieten

Versie: 1.0
Datum: 18-07-2023

Documenthistorie

Versiebeheer

Datum	Versie	Status	Auteur	Wijzigingen
22-11-2022	0.1	Initieel Concept	Tom Driessen en Valesca van Zwieten	Eerste opzet na inventarisatie bestaand beleid en bekende knelpunten
05-12-2022	0.2	Eerste aanvullingen	Tom Driessen en Valesca van Zwieten	Opzet gemaakt van inleiding en eerste beleidsregels gevuld.
27-12-2022	0.3	Aanvullingen op basis van verkregen feedback	Tom Driessen en Valesca van Zwieten	Aanpassing in structuur om verschil in domeinen te verduidelijken en verdere uitwerkingen in beleid
15-02-2023	0.4	Aanvullingen op basis van verkregen feedback	Peter Baltus en Valesca van Zwieten	Roadmap informatie afgesplitst, feedback verwerkt. Afstemming met Marc de Waal over datacenter strategie.
22-03-2023	0.5	Concept versie voor CCC	Peter Baltus en Valesca van Zwieten	Aanvullingen op basis van verkregen feedback
6-4-2023	0.7	Conceptversie voor Ketenoverleg	Peter Baltus en Valesca van Zwieten	Gereed maken voor MT. Hoofdstuk 'Inrichtingsprincipes voor de Amsterdam UMC Azure Cloud' los gekoppeld en addendum van gemaakt.
04-07-2023	0.97	Conceptversie voor MT	Peter Baltus en Valesca van Zwieten	-

Distributie

Datum	Versie	Aan	Functie of rol
12-12-2022	v0.2	Interne review projectgroep	Interne review
09-01-2023	V0.3	MT dag	Ter info
19-01-2023	V0.3	ASB overleg	Interne review
22-03-2023	V0.5	CCC	Interne review en afstemming met standpunten CCC
06-04-2023	V0.6	ASB overleg	Interne review en afstemming
06-04-2023	v0.7	Ketenoverleg Dienst ICT	Interne review en afstemming
17-07-2023	v0.97	MT overleg Dienst ICT	Vaststellen
18-07-2023	v1.0	K2	Publiceren

Referenties

Auteur	Titel	Bron
Laurens Groenewege	VUmc Kaderdocument Clouddiensten v1.0, 28-09-2015	Kwaliteitsnet locatie VUmc
Arie Elsenaar	Beleidskader Cloud-applicaties (SaaS-diensten), v1.0, 21-01-2020	K2
SURF	Juridisch Normenkader (Cloud) services (JNK), 2018	SURF Juridisch Normenkader (Cloud)services | SURF.nl
Ministerie van Binnenlandse Zaken en Koninkrijkrelaties	Kamerbrief Rijksbreed Cloudbeleid 2022	Kamerbrief-over-rijksbreed-Cloudbeleid-2022.pdf

Afkortingen

Afkorting	Definitie
CCC	Cloud Competence Center
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
AAD	Azure Active Directory
CAF	Cloud Adoption Framework
OIDC	OpenID Connect
SAML	Security Assertion Markup Language

Inhoud

1 Inleiding

Dit document geeft kaders en richtlijnen voor toepassing van Clouddiensten binnen Amsterdam UMC. De inleiding licht toe waarom deze kaders nodig zijn.

1.1 Aanleiding

Clouddiensten zijn onderdeel van de informatievoorziening van Amsterdam UMC. Ze worden geleverd door derden en staan fysiek op afstand van waar de organisatie gevestigd is. Door gebruik van Clouddiensten kan Amsterdam UMC flexibel omgaan met rekenkracht, data-opslag en kan het deze diensten afnemen en betalen van per gebruikte eenheid. De laatste paar jaren is de inzet van Clouddiensten in een stroomversnelling geraakt, mede vanwege de trend dat steeds meer applicaties in de Cloud aangeboden worden. Bij de harmonisatie van het applicatielandschap van Amsterdam UMC wordt ook naar Cloudoplossingen gekeken. Een beleidskader dat de actuele vraagstukken bij acceptatie, implementatie, beheer en governance van Clouddiensten behandelt is hierom zeer wenselijk. Daarnaast helpt dit beleidskader met het bouwen van een brug tussen de praktijk en operationele werkzaamheden en biedt het handvatten voor het Cloud Competence Center (CCC).

1.2 Doel en doelgroepen van dit document

De Dienst ICT stelt dit Clouddiensten beleidskader op om Clouddiensten op een gestructureerde en doordachte manier aan te kunnen bieden binnen het Amsterdam UMC. Met dit beleid kunnen Clouddiensten goed geïntegreerd en gebruik worden met het ICT landschap van het Amsterdam UMC.

De doelgroepen van dit document zijn:
- opdrachtgevers, ter ondersteuning bij Clouddiensten;
- ICT-architecten, voor de verwerking in domeinplannen en roadmaps;
- beheerders, als kader voor toetsing, invoering, beheer en beëindiging van Clouddiensten;
- informatiemanagers, als technisch kader bij de inventarisatie van requirements;
- Inkoop en contractmanagement, als kader voor uitwerking en management van contracten.

1.3 Wat wordt er verstaan onder ‘on premises’ en ‘Clouddiensten’?

In dit document wordt met ‘on premises’ bedoeld dat de soft- en hardware die door het Amsterdam UMC in gebruik is, geïnstalleerd is op servers en computers die in eigen beheer en eigendom zijn. Voor een on premises oplossing in het Amsterdam UMC is het niet per se zo dat deze servers en computers op eigen locatie/in het eigen pand aanwezig hoeven te zijn. Dit kan ook een gehuurde locatie zijn. Naast on premises krijgt de Dienst ICT steeds vaker te maken met Clouddiensten. De term “Cloud” wordt toegepast voor een breed scala aan diensten die bij externe partijen kunnen worden afgenomen en via het internet worden geleverd. Het Amerikaanse National Institute of Standards and Technology (NIST) benoemt een aantal typerende kenmerken over Clouddiensten:

- Zelfbediening, "on-demand" af te nemen;
- Breed toegankelijk via netwerken (internet);
- Gedeelde voorzieningen, onafhankelijk van locatie;
- Elastische schaalbaarheid -de mogelijkheid om zeer snel veel meer of minder van de dienst af te nemen;
- Meetbaar verbruik.

Bij Clouddiensten zijn zowel voor- als nadelen die kunnen spelen in het maken bij de afweging of Clouddiensten geschikt zijn om in te zetten. Tabel 1 geeft een aantal voor-en nadelen weer.

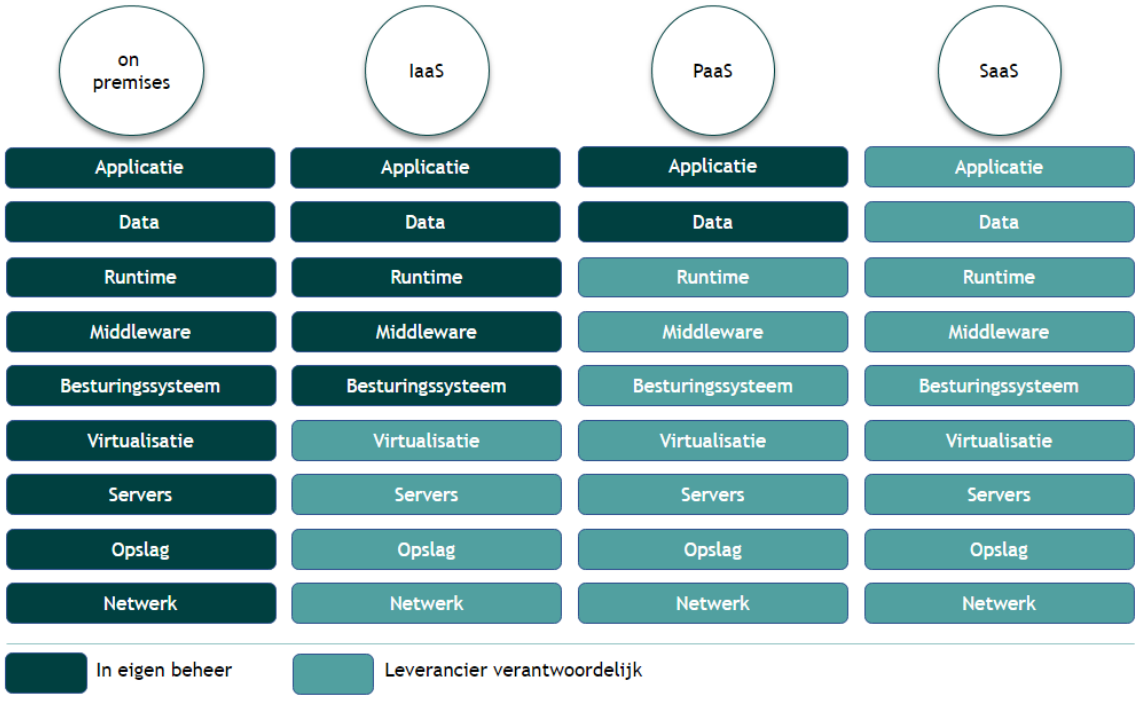
Voordelen	Nadelen
• Snelle levering	• Gegevens beheer/opslag uit handen
• Geen investeringen, maar betaling voor het gebruik	• Afhankelijkheid van netwerk -en internetverbindingen
• Professionele ondersteuning –de schaal waarop de aanbieders werken betekent dat zij veel meer investeren in-en ervaring hebben met-het beschikbaar houden en beveiligen van IT.	• Geen, of complexe integratie met interne systemen • Veeleisend voor de regiefunctie van Amsterdam UMC richting Cloud leveranciers
• Geen noodzaak om zelf een technisch beheer uit te voeren (andere typen functie wel noodzakelijk)[1]	• (Buitenlandse) Wet- en regelgeving mogelijk van toepassing
• Capaciteit op maat	• Intern en extern OTAP beleid mogelijk niet compatible. Aanpassing is dan meestal intern noodzakelijk

Tabel 1. Voor- en nadelen van Clouddiensten.

[1] Voor het deel dat uit handen wordt gegeven is geen technisch beheer nodig, bij IAAS is er vaak wel sprake van technisch beheer.

1.3.1 SOORTEN CLOUDDIENSTEN

Naast de on premises oplossing is het van belang om onderscheid te maken tussen drie service modellen waarop Clouddiensten worden aangeboden. Deze drie modellen zijn: [1] Software as a Service (SaaS), [2] Platform as a Service (PaaS) en [3] Infrastructure as a Service (IaaS). Figuur 1 geeft schematisch weer welke onderdelen zelf ingericht en beheerd kunnen worden als er gekozen wordt voor een van deze Cloud modellen. Beheerverantwoordelijkheid van de leverancier betekent niet dat eigenaarschap (van data) ook bij de leverancier is belegd.



Figuur 1. Schematisch overzicht van verschillende type Cloud modellen en bij behorende onderdelen.[2]

Tabel 2 vat de kernpunten per Cloud model samen en geeft een voorbeeld welke binnen Amsterdam UMC wordt toegepast.

Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
• IT bouwstenen; • Amsterdam UMC verantwoordelijk voor de inrichting van de afgenomen infrastructuur, waar bovenop Amsterdam UMC met (andere) leveranciers applicaties beschikbaar maakt; • ICT infrastructuur beheert de besturingssystemen en stuurt de IaaS leveranciers aan. *Gericht op: Systeembeheerders* *Voorbeeld: Virtuele server via Microsoft Azure*	• "landingsbaan" voor applicaties; • Amsterdam UMC verantwoordelijk voor technisch applicatie beheer bovenop het platform; • Amsterdam UMC stuurt de leveranciers aan. *Gericht op: Ontwikkelaars* *Voorbeeld: SQL Database via Microsoft Azure*	• Compleet functioneel product voor de eindgebruikers; • Amsterdam UMC voert alleen functioneel beheer uit op de dienst inclusief het regie op koppelingen (met on premises omgeving) • Amsterdam UMC stuurt leveranciers aan *Gericht op: Eind gebruikers* *Voorbeeld: E-mail dienst via Microsoft Office 365*

Tabel 2. Kernpunten en voorbeelden binnen Amsterdam UMC per Cloud model.

Er zijn ook nog twee andere vormen van externe ICT dienstverlening die niet onder Clouddiensten gerekend worden:

1. Application Service Provider: De leverancier biedt de applicatie vanaf een externe locatie aan, op een speciaal voor de klant ingerichte infrastructuur, echter zonder de specifieke eigenschappen en voordelen van Clouddiensten.
2. Co-locatie: De leverancier biedt ruimte voor het plaatsen van infrastructuur van de klant. Daarbij zijn de locatie, het gebouw, de netwerktoegang, de elektriciteitsvoorzieningen en de beveiliging geoptimaliseerd voor het grootschalig aanbieden van datacentrum faciliteiten.

1.3.2 BESCHIKBAARHEID VAN CLOUDDIENSTEN

Er zijn verschillende vormen van Clouddiensten:

- **Public Cloud**: de Cloud voorzieningen zijn ingericht voor algemeen en openbaar gebruik. Een (vaak commerciële) partij is eigenaar en beheerder van de dienst;
- **Community Cloud**: de Cloud voorzieningen zijn exclusief voor een groep organisaties ingericht die een gemeenschappelijke missie of doelstelling hebben en vergelijkbare eisen stellen aan de dienst en de informatieveiligheid ervan;
- **Private Cloud**: de Cloud voorzieningen zijn exclusief voor inzet ten behoeve van de eigen organisatie ingericht (waarbij er al dan niet sprake kan zijn van co-locatie). Binnen een private Cloud gaan een aantal voordelen verloren: de schaalbaarheid is beperkt tot de infrastructuur binnen de organisatie zelf en de levertijd is afhankelijk van de intern ingerichte processen. Daar staat tegenover dat de gegevens in eigen beheer blijven, en dat afhankelijk van de implementatie de afhankelijkheid van internet of WAN verbindingen verminderd wordt;
- **Hybride/Multi Cloud**: bij een hybride oplossing worden verschillende van de bovenstaande opties gecombineerd. De omgevingen zijn gescheiden, maar applicaties kunnen door het hanteren van toepasselijke technische standaarden gemakkelijk van de ene naar de andere omgeving overgezet worden.

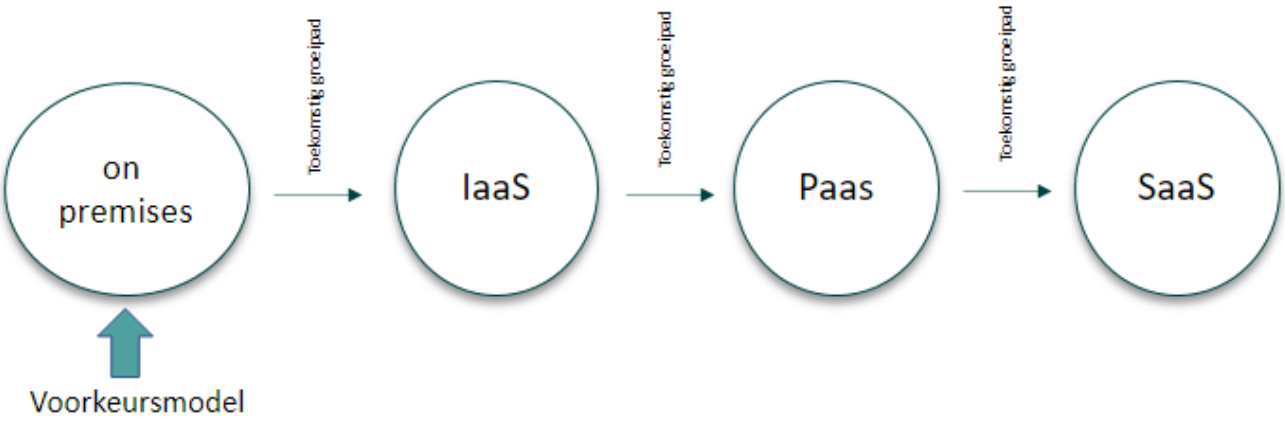
1.4 Adoptie

Amsterdam UMC hanteert een 'Cloud Enabled' Cloudstrategie. Dit houdt in dat Clouddiensten worden gebruikt als dit beter (op het gebied van kosten, beheerlast, snelheid levering, performance, schaalbaarheid, etc.) is voor behalen van de (bedrijfs)doelstellingen. Zo niet dan gaat de voorkeur uit naar on premises IT voorzieningen.

In de bedrijfsvoering van het Amsterdam UMC wordt onderscheid gemaakt tussen verschillende domeinen (figuur 2) die invloed hebben op de keuze voor een bepaalde strategie (Cloud of on premises)

Figuur 2. Schematisch overzicht van strategie voorkeur per bedrijfsdomein

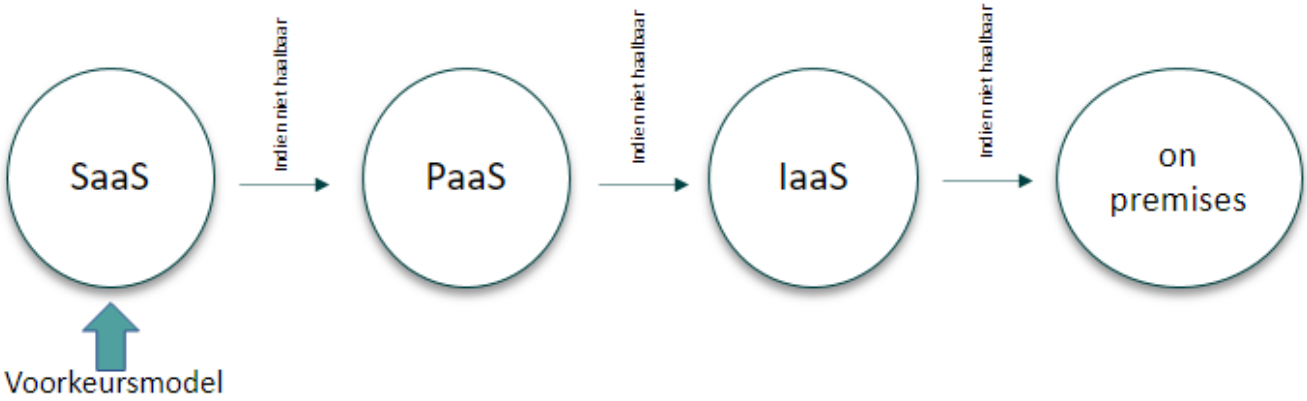
Het zorg domein is van oudsher minder geschikt om selectieve workloads naar de Cloud te verplaatsen. Dit omdat er veel informatie-uitwisseling is tussen systemen. Deze uitwisseling bestaat uit gestructureerde data en beeldmateriaal. Datatransport tussen de Cloud en de on premises infrastructuren kost geld, een hybride infrastructuur is hierdoor erg kostbaar. Ook de beschikbaarheid van Clouddiensten is hier een meewegende factor. Daarom is op dit moment het plaatsen van zorgapplicaties in de on premises datacenters preferent waarbij rekening gehouden wordt met een toekomstig groeipad richting IaaS, vervolgens PaaS en daarna SaaS. Bij de selectie van software is het te adviseren om alvast vereisten mee te geven waardoor het groeipad gevolgd kan worden. Figuur 3 geeft de voorkeur van servicemodellen aan voor het zorg domein.



Figuur 3. Servicemodellen in voorkeur van volgorde voor het zorgdomein.

De aanpak is andersom voor applicaties in de niet-zorg domeinen: bedrijfsvoering, onderwijs en onderzoek. In deze domeinen wordt data meer uitgewisseld in de vorm van datasets en zijn applicaties al in grote mate in SaaS uitvoeringen te verkrijgen. Voor deze domeinen geldt een voorkeur voor Cloud. Wanneer de voorkeur bij een Clouddienst ligt moet er een servicemodel gekozen worden dat hier het best bij past. Tot de Clouddiensten behoren alle mogelijkheden (IaaS, PaaS, of SaaS). Belangrijk bij het maken van de uiteindelijke keuze voor een bepaald servicemodel

is de volgorde waaraan Amsterdam UMC voor het specifieke bedrijfsdomein de voorkeur geeft. Figuur 4 geeft de voorkeur van servicemodellen aan voor het niet-zorg domein.



Figuur 4. Servicemodellen in voorkeur van volgorde voor het niet-zorgdomein.

Aan de keuze voor een servicemodel voor een applicatie liggen meerdere aspecten ten grondslag die hier niet zijn beschreven. De Dienst ICT ondersteunt bij het maken van de juiste keuze.

1.5 Gerelateerd beleid

Dit Clouddiensten beleid staat in relatie met ander beleid, producten en diensten. Integraal van toepassing zijn alle kaders rond privacy en security inclusief AVG-wetgeving en de NEN7510. Binnen de zorg komen daar nog de eisen rond patiëntveiligheid (JCI) en gebruik van medische apparatuur en programmatuur (MDR/IVDR) bij. Verder is al het beleid rond ICT diensten van toepassing; alleen vanwege het feit dat het platform in beheer is bij een externe partij, zijn er extra aandachtspunten. Dit beleid gaat vooral in op die aandachtspunten.

2 Kaders en richtlijnen voor Cloud gebruik

Dit hoofdstuk bevat de kaders en richtlijnen voor Cloud gebruik binnen Amsterdam UMC. Deze kaders en richtlijnen dienen door eenieder gehanteerd worden die met Cloud computing in aanraking komt. Indien het kader of de richtlijn niet passend is dan kan met de Dienst ICT onderzocht worden of afwijking mogelijk is.

2.1 Selectie eisen voor Cloud gebruik

Bij gebruik van Cloud computing wordt een aantal eisen gesteld waar de aanbieder tenminste aan dient te voldoen. Deze selectie eisen zijn:

Principe	**Clouddiensten zijn compliant aan wet- en regelgeving rond privacy en security**
Rationale	Bij gebruik van Cloud services moet de aanbieder bij aanvang en gedurende de gehele periode van gebruik voldoen aan de minimale eisen die gesteld zijn vanuit de wetgever op het thema privacy. Aanvullende regelgeving vanuit Amsterdam UMC vereist ook compliancy met specifieke certificeringen.
Consequenties	Aanbieder is verantwoordelijk om compliant te blijven met wetgeving en voldoet aan ISO27001 en/of NEN7510
Servicemodel	SaaS, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**Wanneer een aanbieder van Clouddiensten voor de levering gebruik maakt van Clouddiensten van derden, dienen deze diensten van derden ook te voldoen aan de eisen van het Amsterdam UMC Cloud beleid.**
Rationale	De volledige oplossing moet voldoen aan wet en regelgeving, de aanbieder is hiervoor verantwoordelijk.
Consequenties	Aanbieder is verantwoordelijk om compliant te blijven met wetgeving en voldoet aan ISO27001 en/of NEN7510
Servicemodel	SaaS, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**Clouddiensten zijn onderdeel van de totale informatievoorziening van Amsterdam UMC.**
Rationale	Het gebruik van Clouddiensten als onderdeel van de totale informatievoorziening van Amsterdam UMC kan voordelen bieden op het gebied van schaalbaarheid, flexibiliteit, kosten, veiligheid, betrouwbaarheid en integratie voor informatie-uitwisseling.
Consequenties	Het Amsterdam UMC beleid voor ICT-diensten is integraal van toepassing op Clouddiensten.
Servicemodel	SaaS, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**Amsterdam UMC houdt het intellectueel eigendom van de data en heeft ten aller tijden toegang tot deze data.**
Rationale	Door het behouden van het intellectueel eigendom van data en de toegang hiertoe kan het Amsterdam UMC controle uitoefenen over hoe de data gebruikt, gedeeld en geanalyseerd wordt.
Consequenties	Enkel Cloud toepassing waarbij expliciet in de voorwaarden vermeld is dat Amsterdam UMC (intellectueel) eigendom en toegang behoudt van zijn data kunnen ingezet worden.
Servicemodel	SaaS, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**Er zijn gestandaardiseerde koppelvlakken voor gegevensuitwisseling**
Rationale	Om consistentie te behouden en uitwisselbaarheid van gegevens te vergemakkelijken moeten Clouddiensten zich conformeren aan de standaard beschikbare koppelvlakken van Amsterdam UMC.
Consequenties	Alvorens te contracteren is het noodzakelijk om te onderzoeken hoe data uitwisseling tussen SaaS <-> On premises systemen en ook tussen SaaS-applicaties via standaard veilige protocollen mogelijk is.
Servicemodel	SaaS, PaaS, IaaS, On premisess
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**Regievoering op Cloud aanbieders wordt ingericht**
Rationale	Aanbieders van Cloud voorzieningen worden aangestuurd via de bestaande Service Management processen om te monitoren dat dienstverlening binnen de kaders en verwachtingen van Amsterdam UMC blijft plaatsvinden.
Consequenties	Bij contractering vindt ook de uitwerking van het Service Management plaats.
Servicemodel	SaaS, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**Opdrachtgevers en gebruikers behouden hun “Single point of contact”**
Rationale	Eenduidige ICT-dienstverlening aan opdrachtgevers en gebruikers, onafhankelijk van een specifieke applicatie, versnelt de afhandeling van vragen en problemen.
Consequenties	De Dienst ICT is de contractpartner. Bij implementatie van de Clouddienst neemt de Dienst ICT het initiatief om de benodigde overlegstructuur in te richten. Daarin zijn opdrachtgever, Dienst ICT en leverancier vertegenwoordigd. Voor bepaalde zaken (denk aan functionele-acceptatieprocessen) zijn rechtstreekse contacten tussen opdrachtgever en leverancier gewenst of zelfs noodzakelijk. De Dienst ICT voert daarover de regie om bij voorkomende problemen snel en adequaat te kunnen handelen. Om het de Dienst ICT mogelijk te maken zijn regierol te kunnen uitvoeren, wordt met de aanbieder van Clouddiensten afgesproken dat zij de Dienst ICT informeren over lopende contacten binnen Amsterdam UMC. Alle zaken die de aanbieder betreffen worden vastgelegd in de overeenkomst.
Servicemodel	SaaS, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**De Clouddienst voldoet aan de eisen vanuit de BIV-classificatie en DPIA**
Rationale	Alle Clouddiensten worden ingericht waarbij maatregelen worden getroffen die passen bij de opgestelde BIV-classificatie. Daarnaast wordt er voor het verwerken van de gegevens een DPIA opgesteld en maatregelen die de gegevens moeten beschermen worden doorgevoerd.
Consequenties	Per Cloud voorziening wordt een BIV-classificatie en een DPIA uitgevoerd.
Servicemodel	SaaS, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**De Clouddienst heeft een exit-strategie**
Rationale	Een exit-strategie zorgt ervoor dat het Amsterdam UMC niet volledig afhankelijk wordt van een specifieke Clouddienst. Een exit-strategie borgt dat het mogelijk is om over te stappen naar een andere leverancier als dit nodig is, zonder grote verstoring of verlies van gegevens.
Consequenties	Onderzoek naar mogelijkheden om de dienst te verlaten moet al in de selectiefase (voor het selecteren van de Clouddienst) geschieden. Onderwerpen waarnaar gekeken moet worden zijn: - Data die verwerkt wordt in de Clouddienst moet in bruikbaar formaat te exporteren zijn ten behoeve van gebruik in alternatieve diensten. - Waarborgen op continuïteit bij Onenigheid over financiële, contractuele voorwaarden - Continuïteitsgaranties bij faillissement leverancier ("voorheen: veiligstelling in Escrow)
Servicemodel	SaaS, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**Voor IaaS en Paas oplossingen is Azure het voorkeursplatform***
Rationale	Er is al ervaring met Azure voor het researchdomein. Daarnaast maken we gebruik van Microsoft365 SaaS-diensten die eenzelfde basis beheerinfrastructuur delen met Azure. Azure ligt daarom voor de hand om hiermee verder mee te werken. De Azure kennis wordt hiermee verder uitgebreid en er hoeft geen verdieping plaats te vinden voor andere Cloudproviders. Op dit moment is er binnen het Amsterdam UMC ook al een groot Microsoft platform, zowel in de Cloud als on premises. * De keuze voor Azure betekent niet dat voor IaaS en PaaS toepassingen automatisch aan de overige eisen in dit document voldaan wordt. Bij ontwerp en implementatie dienen deze eisen nadrukkelijk geadresseerd te worden.
Consequenties	Het gebruik van Azure als voorkeursplatform kan resulteren in een afhankelijkheid van Microsoft als Cloudprovider. Hiermee wordt de flexibiliteit en de mogelijkheid om over te stappen naar een andere Cloudprovider beperkt. Daarnaast kan het uitdagingen met zich mee brengen wanneer er bestaande systemen en applicaties moeten verbinden met de Azure-infrastructuur. Het is van belang om deze consequenties zorgvuldig af te wegen en een weloverwogen beslissing te nemen over het vasthouden aan Azure als het voorkeursplatform.
Servicemodel	PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

2.2 Certificeringen

Principe	**SaaS leveranciers van zorgapplicaties zijn NEN7510 gecertificeerd**
Rationale	De NEN7510 is een norm die specifiek gericht is op informatiebeveiliging in de zorg. Door te stellen dat een leverancier NEN7510 gecertificeerd is, borgt het Amsterdam UMC dat de leverancier voldoet aan de wettelijke (beveiligingsvereisten) vereisten die onder andere relevant zijn voor het beschermen van gevoelige medische gegevens.
Consequenties	Enkel zorgapplicaties van SaaS-leveranciers die een NEN7510 certificaat hebben zijn in te zetten door Amsterdam UMC.
Servicemodel	SaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**SaaS leveranciers zijn ISO27001 gecertificeerd**
Rationale	Het verwerken van (vertrouwelijke) informatie van Amsterdam UMC door een SaaS applicatie vraagt om passende maatregelen om de informatie te beschermen. In de ISO27001 zijn hiervoor normen vastgelegd die Amsterdam UMC als basis vraagt van de SaaS leveranciers.
Consequenties	Enkel applicaties van SaaS-leveranciers die een ISO 27001 certificaat hebben zijn in te zetten door Amsterdam UMC.
Servicemodel	SaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

2.3 Authenticatie en Autorisatie

2.3.1 MEDEWERKER ACCOUNTS

Principe	**Medewerkers accounts worden via het IAM proces gecreëerd**
Rationale	Medewerker accounts zijn accounts die verstrekt worden aan medewerkers van Amsterdam UMC die toegang moet hebben tot digitale informatiesystemen. Dit type account vormt de digitale identiteit van een medewerker en is enkel geschikt voor persoonlijk gebruik. De oorsprong van het medewerkers account is de persoonsregistratie in het HR systeem van Amsterdam UMC. Als een medewerker daarin bekend is wordt het via standaard IAM processen “provisioned” in de identity store van Amsterdam UMC. Als de medewerker de organisatie verlaat wordt het account “deprovisioned”. De identity store is gebaseerd op een on premises uitvoering van Active Directory Domain Services. Vanuit deze identity store wordt er via AD Connect een digitale identity in Azure Active Directory gecreëerd.
Consequenties	Voor medewerkers worden geen accounts handmatig aangemaakt.
Servicemodel	Saas, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**Cloud voorzieningen gebruiken Azure AD als identity store**
Rationale	Door Azure AD als identity store te gebruiken kan het Amsterdam UMC het gebruiksbeheer vereenvoudigen. Het biedt één centrale locatie voor het beheren van gebruikersaccounts, inloggegevens en toegangsrechten, wat het proces van het verlenen en intrekken van toegang vereenvoudigt.
Consequenties	Alle applicaties of voorzieningen die aangeboden worden uit een Clouddienst en die gebruik moeten maken van de Amsterdam UMC digitale identity, gebruiken hiervoor de informatie die aanwezig is in Azure Active Directory.
Servicemodel	Saas, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Zorg

2.3.2 GAST/GUEST ACCOUNTS

Gast accounts enkel online te gebruiken

Principe	**Gastaccounts worden niet via het HR systeem beheerd**
Rationale	Een gastaccount is een account voor toegang tot specifieke diensten voor specifieke personen die niet geregistreerd zijn in het HR systeem. Autorisaties voor gastaccounts zijn beperkt omdat het betrouwbaarheidsniveau van gastaccounts niet gegarandeerd kan worden.
Consequenties	Gastaccounts worden beheerd volgens de Azure B2B of B2C creatiemethodes of SurfConext federatie. Gastaccounts zijn niet te gebruiken op on premises systemen van Amsterdam UMC die gebruik maken van Active Directory voor authenticatie en autorisatie.
Servicemodel	Saas, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**Autorisaties verstrekt aan gastaccounts worden 1 keer per jaar herzien**
Rationale	Een jaarlijkse herziening van gastaccounts is wenselijk om veiligheid te borgen en te blijven voldoen aan wet- en regelgeving betreft gegevensbescherming en privacy. Hiermee wordt ongeautoriseerde toegang tot het systeem of gegevens voorkomen.
Consequenties	De eigenaar van de resource waarvoor het gastaccount verstrekt is herziet de autorisatie.
Servicemodel	Saas, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

2.3.3 FEDERATIEVE AUTHENTICATIE

Federatief inloggen via Azure AD

Principe	**Amsterdam UMC ondersteunt enkel federatief inloggen voor online apps**
Rationale	Federatief inloggen stelt gebruikers instaat om één set inloggegevens te gebruiken om toegang te krijgen tot meerdere onafhankelijken diensten. Medewerkers die inloggen op een SaaS applicatie gebruiken hun Amsterdam UMC digitale identiteit. Op deze manier behoudt Amsterdam UMC meer controle over de accounts in de Cloudapplicaties omdat ze op één centrale plek beheerd worden.
Consequenties	De identiteitscontrole voor de domeinen Zorg en Bedrijfsvoering wordt geregeld door Azure AD. Alle SaaS applicaties worden geregistreerd als Enterprise Application en geconfigureerd voor SAML of OIDC authenticatie.
Servicemodel	SaaS
Bedrijfsdomein	Bedrijfsvoering, Zorg

Federatief inloggen via SurfConext

Principe	**Amsterdam UMC ondersteunt enkel federatief inloggen voor online apps**
Rationale	Medewerkers die inloggen op een SaaS applicatie gebruiken hun Amsterdam UMC digitale identiteit. Op deze manier behoudt Amsterdam UMC meer controle over de accounts in de Cloudapplicaties omdat ze op één centrale plek beheerd worden. Bij onderwijs en onderzoek wordt voor SurfConext gekozen omdat er veel applicaties daar al beschikbaar zijn.
Consequenties	De identiteitscontrole voor de domeinen Onderwijs en Onderzoek wordt geregeld door SurfConext. Alle SaaS applicaties worden gekoppeld via SurfConext en geconfigureerd voor SAML of OIDC authenticatie.
Servicemodel	SaaS
Bedrijfsdomein	Onderwijs, Onderzoek

2.3.4 BEHEERACCOUNTS

Principe	**Admin accounts gebruiken altijd MFA, muv de "break the glass" administrator**
Rationale	Toegang tot systemen met verhoogde permissies zoals die toegekend worden aan een Admin account wordt extra beveiligd door gebruik van Multifactorauthenticatie (MFA). De 'break the glass' accounts worden uitgezonderd van deze beveiliging om in het geval van een storing toch toegang te behouden.
Consequenties	Alle Admin accounts hebben MFA geactiveerd. Voor de 'break the glass' accounts worden andere beveiligingsmaatregelen getroffen vanwege het ontbreken van MFA.
Servicemodel	SaaS, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

3 Technische kaders en richtlijnen voor Cloud gebruik

Dit hoofdstuk bevat technische kaders en richtlijnen voor Cloud gebruik binnen Amsterdam UMC. Indien het kader of de richtlijn niet passend is dan kan via de Cloud Architect van de Dienst ICT van Amsterdam UMC in gezamenlijkheid onderzocht worden of afwijkend maatwerk mogelijk is.

3.1 Authenticatie en Autorisatie

3.1.1 AZURE AD BEHEERACCOUNTS

Principe	**Er worden twee "break the glass" admins gebruikt in de Azure omgeving van Amsterdam UMC**
Rationale	Twee accounts worden aangemaakt om bij configuratie fouten in Conditional Access die ertoe leiden dat alle beheerders buitengesloten worden van beheertaken toch toegang te hebben.
Consequenties	Om configuratie fouten in de Azure omgeving op te mitigeren zijn er 2 global administrator accounts ingericht die geen MFA verplichting hebben. Deze accounts worden gemitigeerd door: 1. het account wordt ingericht met de .onmicrosoft.com UPN; 2. het gebruik van een complex password dat in een password management applicatie wordt vastgelegd; 3. auditing wordt ingericht zodat inloggen met deze accounts gerapporteerd wordt.
Servicemodel	IaaS
Bedrijfsdomein	Bedrijfsvoering

3.1.2 SYSTEEM ACCOUNTS

Principe	**Systeem accounts kennen een Amsterdam UMC eigenaar**
Rationale	Systeem accounts worden in AAD aangemaakt ten behoeve van processen die niet in een eindgebruikerscontext opereren. Omdat er wel iemand verantwoordelijk moet zijn voor het account wordt er een eigenaar toegewezen.
Consequenties	Toegang tot systemen door externe medewerkers worden altijd gekoppeld aan een Amsterdam UMC medewerker die administratief verantwoordelijk is voor het onderhoud van dit account. Er wordt gedocumenteerd welke medewerker aanspreekpunt is voor vragen over een betreffend service account / managed identity.
Servicemodel	SaaS, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**Traditionele service accounts worden gebruikt voor systeemtoegang tot on premises resources**
Rationale	Service accounts worden gebruikt om een applicatie zichzelf te kunnen laten identificeren en aanmelden op het netwerk. Traditionele service accounts worden gebruikt voor toegang tot resources die zich in het on premises netwerk bevinden.
Consequenties	Accounts worden aangemaakt in de lokale AD.
Servicemodel	IaaS
Bedrijfsdomein	Bedrijfsvoering

Principe	**Managed Identities worden gebruikt voor systeemtoegang van Azure resources door Azure workloads**
Rationale	Managed identities helpen het beheer van identiteiten en toegangsbeheer voor applicaties te vereenvoudigen. Zowel system-assigned als user-assigned managed identities worden gebruikt voor toegang tot Azure resources door Azure workload.
Consequenties	Managed Identities worden aangevraagd en beschikbaar gesteld door beheerders.
Servicemodel	SaaS, PaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**Multi tenant apps die Open Authorization 2.0 (Oauth2) ondersteunen worden geregistreerd in de Enterprise App Portal**
Rationale	Alle applicaties die vertrouwd worden door Amsterdam UMC en gebruik mogen maken van informatie uit de AAD worden als Enterprise App geregistreerd. Dit is de werkwijze van Microsoft. Door registratie houdt Amsterdam UMC controle over welke applicaties er toegang hebben tot de gegevens.
Consequenties	Alle apps worden geregistreerd in de Enterprise App portal. Het gebruik van SAML en Oauth2 is hierbij beide toegestaan.
Servicemodel	SaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

3.2 Connectiviteit

3.2.1 ONTSLUITING ON PREMISES -> CLOUD

Principe	**Vaste verbinding met Clouddiensten zijn er enkel voor de Azure Cloud**
Rationale	Amsterdam UMC gebruikt enkel een redundante glasvezelverbinding richting de Azure Cloud (ExpressRoute) via SURF. Overige Cloud aanbieders worden via het publieke internet benaderd. Omdat Azure het voorkeursplatform is wordt alleen voor Azure een permanente en vaste verbinding gerealiseerd.
Consequenties	De verbinding met Azure vanuit het on premises netwerk is beschikbaar en Azure netwerken zijn aanspreekbaar vanuit het on premises netwerk (en vice versa).
Servicemodel	SaaS, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**VPN verbindingen met de Clouddiensten worden getermineerd op de centrale VPN oplossing van Amsterdam UMC**
Rationale	Als er verbindingen benodigd zijn tussen Clouddiensten en het on premises netwerk van Amsterdam UMC voor de ontsluiting van diensten of ten behoeve van applicatie integratie/data uitwisseling dan volgt dit de standaard VPN toepassing die beschikbaar is in het Amsterdam UMC. Op dit moment wil het Amsterdam UMC alle controle uitvoeren voor het netwerkverkeer dat van en naar het Amsterdam UMC komt. Dit centrale knooppunt is momenteel nog intern c.q. in eigen beheer totdat er een keuze is gemaakt om dit op een andere manier te regelen (huidig netwerkbeleid in afwachting van datacenterstrategie).
Consequenties	De standaard centrale Amsterdam UMC VPN oplossing wordt gebruikt voor het koppelen met Clouddiensten.
Servicemodel	Saas, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

3.3 Applicatie integratie

3.3.1 API MANAGEMENT

Principe	**Ontsluiting van applicatie data wordt bij voorkeur gedaan via API ontsluiting. REST heeft daarbij de voorkeur**
Rationale	Een Application Programming Interface (API) is een set van regels en protocollen waarmee verschillende softwaretoepassingen met elkaar kunnen communiceren. Representational State Transfer (REST) is een API architectuurstijl waarbij er aan bepaalde principes voldaan moet worden.
Consequenties	(Nieuwe) Applicaties die data uitwisselen moeten een API interface bevatten waarmee door andere systemen data opgevraagd of aangeleverd kan worden.
Servicemodel	SaaS, PaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

3.3.2 API SECURITY

Principe	**API's van on premises systemen worden ontsloten via een API broker**
Rationale	API verbindingen moeten extra beveiligd worden zodat enkel de geautoriseerde systemen hiermee kunnen communiceren op een door Amsterdam UMC gewenste wijze.
Consequenties	On premises systemen beschikken mogelijk al over een API om data uit te wisselen. De ontsluiting naar Cloud based applicaties verloopt via een API gateway provider die additionele beveiligingsmogelijkheden biedt. *Deze API gateway provider moet nog geselecteerd en geïmplementeerd worden.* Deze wordt gebruikt zodra beschikbaar.
Servicemodel	Saas, PaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

Principe	**Beeldуitwisseling verloopt via API's die FHIR/DICOMweb ondersteunen**
Rationale	Integraties met Cloud systemen die beelden verwerken is mogelijk als deze kunnen koppelen met API interfaces van de beeldsystemen.
Consequenties	SaaS, PaaS applicaties die beelden verwerken moeten uitgerust zijn met een API die FHIR en/of DICOMweb protocollen ondersteunen.
Servicemodel	SaaS, PaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg

3.4 Data backup

Principe	**Applicatiedata in Cloud applicaties is veilig gesteld**
Rationale	Voor data in de Cloud gelden dezelfde eisen als on premises.
Consequenties	Data van Amsterdam die door derden verwerkt worden voldoen minimaal aan de backup/herstel richtlijnen van Amsterdam UMC.
Servicemodel	SaaS, PaaS, IaaS
Bedrijfsdomein	Bedrijfsvoering, Onderzoek, Onderwijs, Zorg