

Bijlage 2 Programma van Eisen

In dit PvE kan de opdrachtnemer zijn aangeduid met "u/uw". Opdrachtgever kan zijn aangeduid met "wij/ons". "Het systeem" is het Citrix-platform dat opdrachtnemer levert onder de opdracht. Het PvE is verdeeld in functionele en non-functionele eisen.

A. Functionele en technische eisen

Nr.	Onderwerp	Eis
A1.	Algemeen	U neemt volledige verantwoordelijkheid voor het technisch beheer van het bestaande Citrix-platform en schakelt hiervoor zonedig met ons als leverancier van de datacentervoorzieningen. In het bijzonder neemt u minimaal de verantwoordelijkheid voor de volgende aspecten: • Onderhoud (lifecycle management) van de Citrix-software op het platform waaronder het periodiek uitvoeren van updates, fixes/patches en releases om daarmee security kwetsbaarheden weg te nemen en gegarandeerd te blijven van support door Citrix. • Onderhoud (lifecycle management) van de virtualisatie- en OS-software op het platform waaronder o.a. het periodiek uitvoeren van updates, fixes/patches en releases om daarmee security kwetsbaarheden weg te nemen en gegarandeerd te blijven van support door Citrix en Microsoft. • Monitoring en optimaliseren van beschikbaarheid, performance en capaciteit van de omgeving en de diensten die daarop draaien.
A2.	Algemeen	U continueert de functionaliteit, performance en security standaarden van het bestaande Citrix-platform zodanig dat de bestaande dienstverlening aan onze studenten, docenten, onderzoekers en overige medewerkers is gewaarborgd. Het Citrix platform bestaat daarbij uit twee deelopgevingen: • Virtuele Apps en Desktop (VAD/shared); • Virtuele Desktop Infrastructure (VDI/non shared). Voor beide deelopgevingen beheert u een afzonderlijk golden image met daarin een verschillende set aan aangeboden applicaties.
A3.	Algemeen	In de aangeboden VAD/shared omgeving kunnen alle applicaties ook als published applicatie aangeboden worden waarbij onderliggend van hetzelfde golden image gebruik gemaakt wordt.
A4.	Koppelingen met onze infrastructuur	De hosting van de on-premises servers van het Citrix-platform vindt plaats in het door ons gecontracteerde datacenter (momenteel KPN/NorthC, locatie Almere) op servers die ons eigendom zijn. Mochten wij besluiten om het Citrix-platform ook te hosten in het secundaire datacenter, dan werkt u hieraan mee. Wij zullen u in dat geval vragen om een offerte voor deze uitbreiding. U kunt deze werkzaamheden uitsluitend uitvoeren na onze schriftelijke goedkeuring van uw offerte.
A5.	Koppelingen met onze infrastructuur	U maakt gebruik van onze SURFnet-internetverbinding. Voor het remote beheer van het Citrix-platform maakt u gebruik van onze VPN-oplossing welke beveiligd is via two-factor authenticatie.
A6.	Koppelingen met onze infrastructuur	U maakt gebruik van de door ons ingekochte Citrix-licenties. Momenteel zijn dit Citrix Universal Hybrid Multi Cloud licenties. Mochten we in de toekomst andere Citrix-licenties inkopen, dan moet u deze gebruiken.

A7.	Koppelingen met onze infrastructuur	Onze gebruikers van de diensten van het Citrix-platform authenticeren via ons Identity & Access Management systeem (momenteel NetIQ) waarbij gebruik gemaakt wordt van onze two-factor authenticatie en de certificate/PKI-omgeving.
A8.	Koppelingen met onze infrastructuur	De toegang tot het Citrix-platform verloopt via onze Citrix ADC/Netscaler (VPX). Wij beheren de Citrix ADC/Netscaler (VPX).
A9.	Koppelingen met onze infrastructuur	U maakt gebruik van de bestaande koppeling met onze Active Directory op basis waarvan policies (GPO) en rechten aan onze gebruikers worden toegekend. Indien wij dit willen, dan vervangt u deze koppeling door een koppeling met onze EntraID. Wij zullen u vragen om een offerte voor deze vervanging. U kunt deze werkzaamheden uitsluitend uitvoeren na onze schriftelijke goedkeuring van uw offerte.
A10.	Koppelingen met onze infrastructuur	De set aan applicaties die specifiek door ons aangewezen gebruikers krijgen aangeboden binnen de VAD/shared en VDI/non shared wordt bepaald en ingesteld door onze beheerders op basis van groepen in onze Active Directory (of in de toekomst EntraID).
A11.	Koppelingen met onze infrastructuur	U maakt gebruik van onze centrale storage omgeving (momenteel Netapp). Deze wordt onder andere gebruikt voor het beschikbaar stellen van gebruikersdata binnen het Citrix-platform (netwerkshares), het wegschrijven van (FSLogix) gebruikersprofielen, het door ons aanleveren van nieuwe applicaties (packages) ter opname in de golden images en het maken van back-ups van de servers door ons.
A12.	Koppelingen met onze infrastructuur	U houdt rekening met de mogelijkheid om het Citrix-platform in de toekomst met cloud servers te koppelen zodat (een deel van) de on-premises Citrix servers vervangen kan worden door Cloud servers. Wij zullen u vragen om een offerte voor deze vervanging. U kunt deze werkzaamheden uitsluitend uitvoeren na onze schriftelijke goedkeuring van uw offerte.
A13.	Koppelingen met onze infrastructuur	U zorgt ervoor dat applicaties die gebruik maken van centrale licentieservers of applicatieservers, hiervoor verbinding maken met de bij ons gehoste centrale servers. Wij zorgen voor het openzetten van noodzakelijke (interne) firewall poorten.
A14.	Gebruikers-functionaliteit	Onze gebruikers kunnen de diensten die vanaf het Citrix-platform geleverd worden benaderen vanaf apparaten met Windows, MacOS, Chrome OS, iOS, Android en de meest gangbare Linux-distributies. Minimaal worden deze diensten ondersteund door de laatste en een-na-laatste versies (n-1) van de Operating Systems. Het Citrix-platform past zich aan de verschillende devices aan, dat wil zeggen 'responsive' pagina's genereren (adaptief design).
A15.	Gebruikers-functionaliteit	Onze gebruikers kunnen het Citrix-platform benaderen door gebruik te maken van de Citrix Workspace App (native). Dit kan zowel als browser plug-in, als zelfstandige app. Minimaal wordt ondersteund de laatste en een-na-laatste versies (n-1) van Chrome, Firefox en Edge.
A16.	Gebruikers-functionaliteit	Onze gebruikers hebben ook de mogelijkheid om het Citrix-platform vanuit alle gangbare browsers via HTML5 te benaderen. Minimaal wordt ondersteund de laatste en een-na-laatste versies (n-1) van Chrome, Firefox en Edge. Dit betreft een Citrix-light variant met verminderde functionaliteit ten opzichte van gebruik van de Citrix Workspace App.

A17.	Gebruikers-functionaliteit	U zorgt dat het portaal (Storefront) van het Citrix-platform qua look and feel aanpasbaar is voor onze huisstijl en biedt tevens de mogelijkheid voor een (tekst) banner waarin voor gebruikers een door ons aangeleverde tekst kan worden geplaatst, zoals de aankondiging van gepland onderhoud.
A18.	Gebruikers-functionaliteit	De virtuele desktop, zowel de VAD/shared als de VDI/non shared, is gebaseerd op een Windows "look and feel".
A19.	Gebruikers-functionaliteit	Gebruikers kunnen printen naar de printqueues in onze infrastructuur en de door de gebruiker ingestelde default printer. Deze queues moeten als printers gevonden worden door de standaard printfunctie van de aangeboden desktop en/of applicatie.
A20.	Gebruikers-functionaliteit	Onze gebruikers van de VAD-omgeving kunnen bestanden openen en opslaan op hun persoonlijke netwerkschijf (U:-schijf), de gezamenlijke netwerkschijf (O:-schijf), OneDrive for Business, Sharepoint, SURFdrive en eventuele faculteit specifieke netwerkschijven.
A21.	Gebruikers-functionaliteit	Gebruikers van de VDI-omgeving kunnen bestanden openen en opslaan op OneDrive for Business, Sharepoint en SURFdrive.
A22.	Gebruikers-functionaliteit	U toont de applicaties binnen het portaal op een gestructureerde wijze aan onze gebruiker, waarbij minimaal drie van de vier onderstaande selecties/indelingen worden ondersteund: • Categorieën. • Zoekmogelijkheid. • Favorieten. • Recent gebruikte applicaties.
A23.	Gebruikers-functionaliteit	De VAD-omgeving maakt interactie (zoals bijvoorbeeld copy-paste en data-opslag) mogelijk tussen applicaties aangeboden vanuit het Citrix-platform en applicaties vanuit een andere bron binnen hetzelfde device (bijvoorbeeld lokaal geïnstalleerde applicaties en de harde schijf van het device). Voor de VDI-omgeving is deze interactie niet beschikbaar.
A24.	Technische eisen	U verricht minimaal twee keer per jaar een restore test van de server back-ups die door ons op dagelijkse basis worden gemaakt. Bij het niet slagen van de test worden in samenwerking met ons correctieve maatregelen genomen totdat de restore test succesvol is.
A25.	Technische eisen	U maakt in overleg met ons en binnen onze randvoorwaarden een disaster recovery plan welke op ons verzoek wordt getest. U levert uiterlijk een half jaar na transitie een uitgewerkt disaster recovery plan op. De Universiteit Utrecht moet het 'disaster recovery plan' goedkeuren voordat het disaster recovery plan definitief is. Wij kunnen bindende instructies geven als voorwaarde voor goedkeuring, die u vervolgens moet doorvoeren in uw disaster recovery plan.
A26.	Technische eisen	U zorgt dat het te beheren Citrix-platform voorzien is (blijft) van de workspace managementoplossing (momenteel Citrix WEM). Onze beheerders (applicatie-packagers) hebben toegang tot deze omgeving zodat zij hiermee tenminste de volgende beheertaken kunnen uitvoeren: • Opslaan van gebruikers- en applicatie-instellingen (profielenbeheer); • Specifieke gebruikers- en applicatie-instellingen uitsluiten of toevoegen (polities, powershell, etc.); • Locatie-onafhankelijk beschikbaar stellen van deze gebruikers- en

		- applicatie-instellingen; - Beheren en inrichten van startmenu's en desktops; - Aanbieden van drive mappings (naar onze storage); - Aanbieden van koppelingen met onze printers; - Aanbieden van koppelingen met door ons beheerde licentie- of applicatieservers; - Aanbieden van applicaties/snelkoppelingen en policies.
A27.	Technische eisen	We willen wijzigingen in het Citrix-platform kunnen testen. Er zijn daarvoor afzonderlijke Test (T-omgevingen) en Acceptatie-omgevingen (A-omgevingen) voor zowel de VAD/shared als de VDI/non shared die door u beheerd worden. Voor deze T- en A-omgevingen geldt: - Ze maken gebruik van dezelfde Citrix management omgeving als de P-omgevingen. - Ze zijn zoveel als mogelijk gescheiden van de P-omgevingen. - Ze hoeven slechts voor een klein aantal concurrent gebruikers (maximaal 10), zoals beheerders, testers en acceptanten, geschikt te zijn. - Ze dienen qua functionaliteit en performance wel representatief te zijn voor de P-omgevingen.
A28.	Technische eisen	U borgt het technisch gelijk houden van de Acceptatie- en Productie-omgevingen, met uitzondering van voorgenomen wijzigingen in de Productie-omgevingen welke reeds succesvol zijn getest in de Test-omgevingen.
A29.	Technische eisen	Behalve P-omgevingen, A-omgevingen en T-omgevingen beheert u ook een ontwikkelomgeving (O-omgeving). Voor deze O-omgeving geldt: - Deze maakt gebruik van dezelfde Citrix management omgeving als de P-omgevingen. - Deze is zoveel als mogelijk gescheiden van de P-omgevingen. - Deze is bedoeld voor onze packagers om zelf applicaties op te installeren. In tegenstelling tot de Productie, Acceptatie en Test-omgevingen is dit een persistent omgeving. - Deze hoeft slechts voor een klein aantal concurrent gebruikers (maximaal 5), namelijk onze beheerders/ packagers, geschikt te zijn. - Deze dient qua functionaliteit en performance wel representatief te zijn voor de P-omgevingen.
A30.	Technische eisen	U maakt gebruik van de FSLogix-oplossing voor het beschikbaar maken van de M365-applicaties, inclusief Onedrive met synchronisatiefunctie. De FSLogix-profielen worden opgeslagen op onze storage-omgeving (een share).
A31.	Technische eisen	De tijdsduur voor automatisch termineren van een Citrix-gebruikerssessie kan voor beiden omgevingen (VAD/shared en VDI/non shared) afzonderlijk worden ingesteld.
A32.	Technische eisen	Binnen de VDI-omgeving wordt de volledige capaciteit van een desktop toegewezen aan één gebruiker op het moment dat deze is gekoppeld (non shared).
A33.	Technische eisen	Elke VDI-gebruiker krijgt per sessie de beschikking over een tijdelijke persoonlijke opslagschijf (werkschijf) met een gegarandeerde omvang, zie bijlage 4 Overzicht fysieke en virtuele servers.
A34.	Technische eisen	De VDI-omgeving heeft de mogelijkheid om voor de bestaande of nieuwe onderzoeksgroep de twee vaste desktop configuraties in de toekomst uit te breiden met nieuwe configuraties in termen van

		toegekende resources (CPU, memory, omvang werkschijf). Een dergelijke aanpassing zal op ons verzoek en in afstemming met ons plaatsvinden. Wij zullen u vragen om een offerte voor deze aanpassing. U kunt deze aanpassing uitsluitend uitvoeren na onze schriftelijke goedkeuring van uw offerte. Wij stellen eventueel noodzakelijke additionele hardware ter beschikking.
A35.	Technische eisen	Onze beheerders hebben gedetailleerd inzage in het gebruik (gebruikerssessies) van het Citrix-platform (zowel VAD/shared als VDI/non shared) en de aangeboden applicaties. U verschaft ons toegang tot alle relevante logfiles, zodat wij hieruit zelf rapportages over het gebruik van het Citrix-platform kunnen samenstellen.
A36.	Applicaties en golden images	Het Citrix-platform is geschikt voor de levering van alle bestaande applicaties die momenteel via het huidige Citrix-platform (VAD/shared en VDI/non shared) geleverd worden, zie Bijlage 5 Applicatie-overzicht (juli 2026). Bijlage 5 betreft een momentopname. Zoals in eis D2 is aangegeven vindt de overdracht van het beheer van het Citrix-platform van de huidige leverancier naar u plaats op 11 oktober 2027. Dit betekent dat er nog diverse wijzigingen plaatsvinden in het applicatie-overzicht voordat u het beheer van het Citrix-platform overneemt. Dit gaat via het "golden image", zie eis A39. U gaat hiermee akkoord.
A37.	Applicaties en golden images	Het Citrix-platform is geschikt voor het in het gebruikersportaal aanbieden van URL's naar SaaS-applicaties, downloadbare content, etc.
A38.	Applicaties en golden images	Wij leveren packages aan welke u aanbiedt in de twee golden images voor respectievelijk de VAD/shared en de VDI/not shared omgeving. De packages blijven ons eigendom.
A39.	Applicaties en golden images	U rolt één keer per maand een nieuw "golden image" uit. U richt daartoe in afstemming met ons een maandelijks proces in voor het vernieuwen van de golden images ten behoeve van het aanbieden van nieuwe (versies van) applicaties. De door ons gewenste wijzigingen in (versies van) applicaties concentreren zich hoofdzakelijk, maar niet uitsluitend, op twee momenten in het jaar, de zogenaamde winter- en zomerrelease (voor de start van nieuwe onderwijsblokken). In de overige maanden blijft het aantal gewenste mutaties vanuit ons beperkt tot gemiddeld drie.
A40.	Applicaties en golden images	In aanvulling op de door ons gewenste wijzigingen in de golden images neemt u daar de volgende onderdelen in mee: • Maandelijks Microsoft patches/fixes (die beschikbaar komen op 'Patch Tuesday'). • Maandelijks updates van de binnen de SolisWorkspace aangeboden browsers inclusief Edge Webview. • Maandelijks updates van de binnen de SolisWorkspace aangeboden M365-applicaties inclusief Onedrive en een beperkt aantal (algemene) applicaties waaronder Adobe Reader. • Updates voortvloeiend uit (Citrix) release management (bijvoorbeeld VDA agent) en andere beheertools (zoals de antivirus agent).
A41.	Applicaties en golden images	U voert op incidentele basis, buiten het maandelijks vernieuwingsproces van golden images om, op ons verzoek een spoedaanpassing in een golden image door (image "openbreken").

A42.	Capaciteit en performance	U zorgt ervoor dat het Citrix-platform geschikt is voor de gebruikersaantallen zoals genoemd in bijlage 4 Overzicht fysieke en virtuele servers.
A43.	Capaciteit en performance	In de periode van 1 oktober 2027 tot en met 15 oktober 2027 wordt een gemiddelde baseline performance vastgesteld op verschillende tijdstippen van de dag. U garandeert dat het te beheren Citrix-platform zodanig geconfigureerd is dat – met een zelfde hardware capaciteit - de gemiddelde baseline performance minimaal gehandhaafd blijft. De volgende componenten maken deel uit van de baseline: • Inloggen op de omgeving vanaf het moment van het ingeven van de two-factor authenticatie tot en met een beschikbare storefront met snelkoppelingen • Doorlooptijd van het volledig opstarten van de volgende key-applicaties vanaf het moment van aanklikken: GLIMS, Nvivo, Jasp, Excel (inclusief plugins) en StataBE. • Muisbewegingen dienen zonder vertraging te verlopen en muisklikken dienen uitgelijnd te zijn.
A44.	Samenwerking met andere leveranciers	U werkt samen met andere leveranciers van ons, als dat de gevraagde dienstverlening ten goede kan komen.

B. Architectuur

Nr.	Onderwerp	Eis
B1.	Architectuur	U werkt onder architectuur conform onze geldende architectuurkaders en ondersteunt onze architect bij het opstellen van een Project Initiative (soort Project Start Architectuur).
B2.	Architectuur	U garandeert dat u informatie over de architectuur, werking en inrichting van alle relevante software en hardwarecomponenten, die onderdeel uitmaken van het Citrix-platform vastlegt, bijhoudt en deelt met ons.
B3.	Architectuur	U borgt dat de door ons aangewezen personen (onder andere Architect, Productowner en functioneel beheerders/ packagers) inzicht krijgen in de technische opbouw van alle relevante componenten, interfaces, datamodellen, beveiliging en technische informatie (waaronder technisch ontwerp en technische White papers). Deze informatie is ons eigendom.

C. Samenwerking

Nr.	Onderwerp	Eis
C1.	Taal	Alle communicatie tussen U en ons (schriftelijk en mondeling) vindt in de Nederlandse taal plaats.
C2.	Service Management	U accepteert de door ons gehanteerde Servicetijd. Dit is de periode dat de u directe ondersteuning biedt in het oplossen van storingen, vragen en (service)verzoeken en daarmee de beschikbaarheid van diensten kan ondersteunen. De Standaard Servicetijd is: • Maandag t/m vrijdag: 08.00 – 17:30 uur. Aanvullend geldt specifiek voor prioriteit 1 storingen de volgende (Verruimde) Servicetijd:

		- Maandag t/m vrijdag: 08.00 – 21:30 uur - Zaterdag, zondag en feestdagen: 10.00 - 18.00 uur.
C3.	Service Management	U accepteert de door ons gehanteerde prioriteitsomschrijving voor een prioriteit 1 storing. Een prioriteit 1 storing is een ernstige verstoring van de dienstverlening. Dit betreft het niet beschikbaar zijn van het Citrix-platform, of één van de afzonderlijke delen: Virtuele Apps en Desktop (VAD/shared) of de Virtuele Desktop Infrastructure (VDI/non shared). Ook het niet beschikbaar zijn van bedrijfskritische applicaties (waaronder GLIMS), als onderdeel van de VAD/shared omgeving, betreft een prioriteit 1 storing.
C4.	Service Management	U gaat akkoord met de volgende maximale functiehersteltijden (inclusief de reactietijden): Prioriteit 1 storingen: vier (4) uur. Deze tijd moet u in 90% van de gevallen halen.
C5.	Service Management	U garandeert gedurende de verruimde Servicetijd, dat wil zeggen de Servicetijd die voor prioriteit 1 storingen geldt, een minimale beschikbaarheid per maand van 99,5%. De beschikbaarheid wordt hierbij berekend met behulp van de volgende formule: $\text{Beschikbaarheid} = (\text{Verruimde Servicetijd} - \text{tijd dienst onbeschikbaar gedurende Verruimde Servicetijd}) / (\text{Verruimde Servicetijd})$ - Onbeschikbaarheid wordt gedefinieerd als de doorlooptijd van een prioriteit 1 storing. - De gerealiseerde beschikbaarheid wordt dus niet over 7x24 uur gemeten, maar over de gedefinieerde Verruimde Servicetijd. Onbeschikbaarheid als gevolg van een tekortkoming van ons of één van onze andere leveranciers, wordt niet meegenomen in de berekening van de beschikbaarheid. Dit gaat dus niet ten koste van de beschikbaarheid (u mag deze tijd als "beschikbaar" rapporteren). Voorbeelden hiervan zijn de uitval van ons datacenter, uitval van ons IAM-systeem of een probleem met de door ons geleverde licenties.
C6.	Service Management	Buiten de genoemde Verruimde Servicetijd moet u het Citrix-platform leveren (openstellen) zodat gebruikers er 7x24 uur gebruik van kunnen maken met uitzondering van gepland en door ons goedgekeurd onderhoud.
C7.	Service Management	U biedt ten behoeve van het melden van storingen, vragen en (service) verzoeken gedurende Standaard Servicetijd een Nederlandssprekende derdelijns ondersteuning (Servicedesk). Specifiek voor prioriteit 1 storingen is derdelijns ondersteuning gedurende de Verruimde Servicetijd beschikbaar.
C8.	Service Management	U zorgt ervoor dat storingsmeldingen elektronisch (via e-mail of website) met ons worden uitgewisseld. Iedere storingsmelding heeft een uniek kenmerk.
C9.	Service Management	U informeert onze Servicedesk en Productowner zo spoedig mogelijk bij constatering van een prioriteit 1 storing vanuit de monitoring(systemen).
C10.	Service Management	U meldt spoedonderhoud aan het Citrix-platform direct bij ons. In uw melding geeft u de verwachte impact op ons aan.
C11.	Service Management	U draagt de 'end-to-end' verantwoordelijkheid voor de volledige oplossing en coördinatie van door ons aangemelde incidenten en

		rapporteert over de voortgang hiervan bij onze Servicedesk en Productowner die het incident heeft aangemeld.
C12.	Service Management	U levert na elke prioriteit 1 storing binnen vijf (5) werkdagen een rapport op (major incident rapport, MIR) met daarin een beschrijving van de oorzaak van de storing, de uitgevoerde actie om de storing op te lossen en waar mogelijk een beschrijving van maatregelen die u heeft genomen om herhaling te voorkomen.
C13.	Service Management	U garandeert dat wijzigingen aan het Citrix-platform eerst worden getest op de Test- en Acceptatieomgevingen.
C14.	Service Management	U garandeert dat alle wijzigingen in de Productie-omgevingen die merkbare gevolgen hebben voor de gebruiker c.q. een functionele impact hebben voor de gebruiker, pas worden doorgevoerd na onze goedkeuring.
C15.	Service Management	U accepteert dat onderhoud aan het Citrix- (Productie) platform dat impact heeft voor gebruikers in principe buiten de Verruimde Servicetijd, dat wil zeggen buiten de Servicetijd voor prioriteit 1 storingen, plaatsvindt, tenzij er sprake is van spoed. In alle gevallen is onze goedkeuring nodig voordat u het onderhoud mag uitvoeren.
C16.	Service Management	U kondigt onderhoud dat impact heeft voor de gebruikers minimaal tien (10) werkdagen van tevoren aan bij ons.
C17.	Service Management	U voert in het maandelijkse vernieuwingsproces van de golden images in afstemming met ons een aantal basale controles uit op de goede werking van nieuwe golden images voordat deze in de Test-omgevingen worden opgeleverd.
C18.	Service Management	U levert de maandelijkse golden images in 80% van de gevallen binnen acht (8) werkdagen in de Test-omgevingen na aanvraag door ons.
C19.	Service Management	U neemt geconstateerde bevindingen in nieuwe golden images - als gevolg van regressietesten door ons - in 80% van de gevallen binnen vijf (5) werkdagen weg.
C20.	Service Management	U zet na ons akkoord in 80% van de gevallen binnen 1 werkdag nieuwe golden images door vanuit de Test-omgevingen naar respectievelijk de Acceptatie- en Productieomgevingen.
C21.	Service Management	U hanteert een standaard procedure (escalatieprocedure) die gevolgd kan worden in geval van het niet nakomen van de verplichtingen onder de overeenkomst, dan wel onduidelijkheid over de te volgen procedure hieromtrent.
C22.	Service Management	U verstrekt op maandelijkse basis, uiterlijk elke tiende (10e) werkdag van de maand, in elektronische vorm een service level rapportage aan ons. In deze maandrapportage is aangegeven in welke mate u heeft voldaan aan de service levels zoals hierboven beschreven en vastgelegd in de SLA.
C23.	Service Management	U evalueert de dienstverlening periodiek (minimaal jaarlijks) samen met ons en stelt op basis van die evaluaties verbeterplannen op en voert deze door.
C24.	Service Management	Wijzigingen geeft u direct door aan de contract- en leveranciersmanager van de opdrachtgever. Enkele voorbeelden hiervan zijn: • Naamswijzigingen.

		• Adreswijzigingen. • Wijziging van accountmanager/contactpersoon. • Wijzigingen in het door u ingezette personeel.
C25.	Service Management	Minimaal één maand voor het begin van de livegang levert u een Service Level Agreement (SLA) aan. De SLA is gebaseerd op uw antwoord in uw inschrijving op G2.5 in bijlage 6, tenzij wij en u wijzigingen overeenkomen. De Universiteit Utrecht moet de definitieve SLA goedkeuren voordat u deze SLA kunt gebruiken.
C26.	Governance	U zal tijdens de looptijd van de overeenkomst met ons de communicatie en overlegstructuur op zowel strategisch, tactisch als operationeel niveau inrichten om de dienstverlening en samenwerking tussen partijen zo goed mogelijk te laten verlopen.
C27.	Governance	U wijst gedurende de looptijd van de overeenkomst op zowel strategisch, tactisch als operationeel niveau vaste contactpersonen met kennis van zaken en mandaat aan. Ieder niveau wordt vertegenwoordigd door een afgevaardigde van ons die specifiek daartoe aangewezen is. U zorgt bij afwezigheid van uw vaste contactpersoon voor een vervanger met kennis van zaken en mandaat. Communicatie op genoemde niveaus vindt alleen tussen de daarvoor bevoegde contactpersonen plaats.
C28.	Governance	Op operationeel niveau vindt minimaal één keer per maand een overleg plaats. Op tactisch en strategisch niveau wordt de frequentie naar behoefte ingevuld.
C29.	Consultancy en Meerwerk	U bent verplicht om ons van advies/consultancy te voorzien inzake technische mogelijkheden van het Citrix-platform en/of relevante nieuwe ontwikkelingen in de markt. U brengt hiervoor geen extra kosten in rekening. Wanneer wij op basis van uw advies/consultancy een schriftelijke opdracht geven is er de mogelijkheid om een strippenkaart-constructie af te nemen. Hierbij hanteert u het vaste uurtarief zoals aangeboden in uw inschrijving. U kunt deze werkzaamheden uitsluitend uitvoeren na onze schriftelijke goedkeuring.
C30.	Consultancy en Meerwerk	U voorziet in de mogelijkheid om door ons gewenste wijzigingen op het Citrix-platform door te voeren. Dit kunnen wijzigingen van diverse aard zijn, bijvoorbeeld als gevolg van wijzigingen in onze aanpalende infrastructuur, gewenste functionele wijzigingen of wijzigingen in de capaciteit van het Citrix-platform. Dit type wijzigingen wordt verrekend conform de vaste uurtarieven, zoals aangeboden in uw inschrijving. Wij zullen u vragen om een offerte. U kunt deze werkzaamheden uitsluitend uitvoeren na onze schriftelijke goedkeuring van uw offerte.
C31.	Consultancy en Meerwerk	U richt in afstemming met ons een proces in om gewenste Meerwerk wijzigingen af te stemmen en door te voeren op het Citrix-platform.

D. Transitie

Nr.	Onderwerp	Eis
D1.	Transitie	U levert in overleg met de Universiteit Utrecht na de ingangsdatum van de opdracht zo spoedig mogelijk (maar uiterlijk binnen twee weken) een 'compleet transitieplan'. Hierin zijn opgenomen alle fasen, inclusief de activiteiten en volgorde, rollen en verantwoordelijkheden, en een tijdsplanning inclusief geplande inspanning van u, de Universiteit Utrecht en onze huidige leverancier voor de transitie. Het transitieplan is gebaseerd op uw antwoord in uw inschrijving op wens G2.1 in bijlage 6, tenzij de Universiteit Utrecht en u wijzigingen overeenkomen. De Universiteit Utrecht moet het 'complete transitieplan' goedkeuren voordat u kunt starten met de transitieplan. Wij kunnen bindende instructies geven als voorwaarde voor goedkeuring, die u vervolgens moet doorvoeren in uw transitieplan. De kosten voor de inzet van uw medewerkers, verwerkt u in uw tarief voor de transitie in het prijzenblad (Formulier C). Dit geldt overigens voor alle kosten in verband met de transitie.
D2.	Transitie	De overdracht van het beheer van het Citrix-platform van de huidige leverancier naar u vindt plaats op 11 oktober 2027. Twee weken voor deze datum geven wij officieel een "go/ no go" aan. Bij een "go" vindt de overdracht plaats op 11 oktober 2027. Bij een "no go" wordt de overdracht uitgesteld tot een nader door ons te bepalen datum. Wanneer het Citrix-platform in de periode van twee weken na overdracht van het beheer stabiel heeft gedraaid, vindt de officiële acceptatie van de overdracht door ons plaats. Mocht het Citrix-platform niet stabiel hebben gedraaid, dan verhelpt u de gebreken binnen 5 werkdagen. Hierna gaat een nieuwe periode van twee weken in waarin het Citrix-platform stabiel moet hebben gedraaid. De termijnen in deze eis zijn fatale termijnen. In uitzonderingssituaties kunnen wij verlenging van de genoemde termijnen toestaan, zonder dat dit tot extra kosten zal leiden voor ons.
D3.	Transitie	Projectmedewerkers worden vanaf de goedkeuring van het transitieplan opgeleid en voorzien van de benodigde kennis van het Citrix-platform. Bij voorkeur wordt het 'voordoen, samen doen, zelf doen' model toegepast en worden de projectmedewerkers in staat gebracht om zelf andere medewerkers te trainen (volgens het train-the-trainer principe).
D4.	Transitie	U stelt een projectleider/programmamanager aan als aanspreekpunt voor ons.
D5.	Transitie	De transitiefase start uiterlijk direct nadat wij het 'complete transitieplan' hebben goedgekeurd.
D6.	Transitie	U garandeert dat de resources zoals beschreven in het 'complete transitieplan' aantoonbaar ervaren zijn, beschikbaar zijn en beschikbaar blijven tot de formele acceptatie van de volledige transitie (inclusief eventuele nazorg) door de Universiteit Utrecht. U vraagt toestemming aan ons als u medewerkers gedurende het project wil vervangen, de vervangende medewerker dient minimaal vergelijkbare ervaring te hebben.

D7.	Re-transitieplan	U levert uiterlijk een half jaar na transitie een uitgewerkt re-transitieplan op, ten behoeve van de afloop of (gedeeltelijke) tussentijdse beëindiging van de overeenkomst. Partijen maken nadere afspraken over de re-transitie. De Universiteit Utrecht moet het 're-transitieplan' goedkeuren voordat het re-transitieplan definitief is. Wij kunnen bindende instructies geven als voorwaarde voor goedkeuring, die u vervolgens moet doorvoeren in uw re-transitieplan. U garandeert dat u meewerkt aan de re-transitie. Daarnaast garandeert u dat de resources die nodig zijn om het 're-transitieplan' uit te voeren beschikbaar zijn en beschikbaar blijven tot de formele acceptatie van de re-transitie door de Universiteit Utrecht.
------------	------------------	--

E. Informatiebeveiliging

Nr.	Onderwerp	Eis
E1.	IB 03 Logging	03.1 Activiteiten die relevant zijn voor de beveiliging (BIV) van gegevens worden gelogd. Opdrachtnemer beschikt over logging waarmee inzicht wordt verkregen in beheeractiviteiten (waaronder authenticatiepogingen), uitgevoerd door de (functioneel en technisch) beheerder. 03.2 Logregels bevatten minimaal een timestamp, een gebruikers-ID (of de identificerende eigenschappen van oorsprong zoals IP-adres), het systeem dat de regel heeft gegenereerd en de uitgevoerde activiteit. 03.3 De in eis IB 03.1 en eis IB 03.2 genoemde logging en overige detail logging dient beschikbaar te zijn voor incidenten en probleemonderzoek. Opdrachtnemer dient bij incidenten en problemen op verzoek van Opdrachtgever meer dan alleen de verkeersgegevens te loggen. De logging dient op verzoek beschikbaar te zijn voor enkel de geautoriseerde gebruikers van Opdrachtgever (bijv. het Security-team), die deze loggegevens moeten kunnen inzien of doorsturen voor informatiebeveiligingsdoeleinden, bijvoorbeeld aan de politie of andere bevoegde (opsporings-)organen. 03.4 NTP of NT5DS wordt gebruikt om de timestamp van de logregels te synchroniseren naar een centrale tijdserver met gps-ontvanger volgens internationale UTC-tijdstandaard. Timestamps zijn vastgelegd in de lokale tijdzone met juiste DST-aanduiding of zijn in ISO 8601 notatie vastgelegd.
E2.	IB 07 Versleuteling (verbindingen en dataopslag)	07.1 Opdrachtnemer zorgt ervoor dat data (inclusief back-up data) van Opdrachtgever versleuteld getransporteerd en opgeslagen worden. 07.2 Opdrachtnemer dient bij het ontsluiten van online omgevingen te allen tijde te zorgen dat gegevensoverdracht is versleuteld. Daarnaast dient de authenticiteit van de verzender en de integriteit van de verzonden data te worden gegarandeerd, waar mogelijk door het gebruik van certificaten. 07.3 Versleuteling voor transport moet gedurende de gehele looptijd van de Overeenkomst voldoen aan de meest recente ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van het NCSC (zie https://www.ncsc.nl) op niveau 'Voldoende' of beter.

		07.4 Opdrachtnemer dient gegevens van Opdrachtgever versleuteld op te slaan volgens minimaal de AES256 standaard.												
E3.	IB 08 Kwetsbaarheden- management	08.1 Opdrachtnemer schat geïdentificeerde kwetsbaarheden in volgens de Common Vulnerability Scoring System (CVSS). Opdrachtnemer zal kwetsbaarheden oplossen volgens de volgende maximale oplostijden: <table border="1"> <thead> <tr> <th>Risicobeoordeling</th><th>CVSS</th><th>Maximale oplostijd</th></tr> </thead> <tbody> <tr> <td>Kritiek</td><td>7 - 10</td><td>5 werkdagen</td></tr> <tr> <td>Hoog</td><td>4 - 6.9</td><td>1 maand</td></tr> <tr> <td>Medium</td><td>0 - 3.9</td><td>3 maanden</td></tr> </tbody> </table> 08.2 Kwetsbaarheden dienen met een permanent fix opgelost te worden. Een eventuele workaround is enkel na goedkeuring van Opdrachtgever mogelijk. 08.3 Bij alle risico's voor Opdrachtgever van Medium of hoger dient Opdrachtnemer de Opdrachtgever direct te informeren over het bestaan van een kwetsbaarheid met een risico voor Opdrachtgever. Deze waarschuwing dient voorzien te zijn van een (voorlopige) inschatting van het risico dat Opdrachtgever loopt, de verwachte oplostijd en welke stappen Opdrachtgever zelf kan nemen om risico's te mitigeren. 08.4 Opdrachtnemer zal security issues van andere klanten die ook van toepassing zijn of kunnen zijn op Opdrachtgever of op enigerlei wijze gevolgen kunnen hebben voor Opdrachtgever met de prioriteit als genoemd in eis IB 08.1 afhandelen.	Risicobeoordeling	CVSS	Maximale oplostijd	Kritiek	7 - 10	5 werkdagen	Hoog	4 - 6.9	1 maand	Medium	0 - 3.9	3 maanden
Risicobeoordeling	CVSS	Maximale oplostijd												
Kritiek	7 - 10	5 werkdagen												
Hoog	4 - 6.9	1 maand												
Medium	0 - 3.9	3 maanden												
E4.	IB 14 Penetratietest (pentest)	14.1 U verleent volledige medewerking aan pentesten die door ons of in opdracht van ons uitgevoerd worden op ons Citrix-platform.												
E5.	IB 23 Kunstmatige intelligentie (AI)	Wanneer kunstmatige intelligentie (AI) ingezet wordt bij, of onderdeel is van het Citrix-platform dient dit te gebeuren op een manier die de beschikbaarheid, integriteit, en vertrouwelijkheid van de data en het systeem niet in gevaar brengt. Hiervoor dient aan de volgende eisen voldaan te worden: 23.1 Een model dat (mede) door andere klanten gebruikt wordt mag nimmer getraind worden op de data van de Opdrachtgever. 23.2 De AI -agent mag geen informatie verschaffen aan gebruikers die deze informatie ook niet via een regulier actie kunnen verkrijgen. 23.3 Een AI-agent mag geen informatie aanpassen/verwijderen in opdracht van een gebruiker die via een reguliere actie deze informatie niet aan mag passen/verwijderen. Dit geldt ook voor het toekennen, aanpassen, en intrekken van rechten. 23.4 Een AI-agent mag in opdracht van een gebruiker geen acties uitvoeren welke de gebruiker via de reguliere weg niet uit mag voeren. 23.5 Indien data gewijzigd wordt, of acties uitgevoerd worden door een AI-agent in opdracht van een gebruiker, dan dient er gelogd te worden wat de opdracht was die de gebruiker heeft gegeven, welke gebruiker de opdracht heeft gegeven, en welke actie de AI-agent uitgevoerd heeft. 23.6 Informatie moet aangemerkt kunnen worden als ontoegankelijk voor AI-agents/modellen waarbij deze geen lees/bewerkingsrechten hebben op deze informatie.												

E6.	IB 24 Informatietoegang	Informatie van de Opdrachtgever mag alleen toegankelijk zijn voor door de Opdrachtgever aangewezen geautoriseerde personen en entiteiten.
E7.	Verklaring omtrent het gedrag (VOG)	Uw personeel dat toegang heeft, of de rechten heeft om toegang te krijgen, tot onze omgeving/ data dient te beschikken over een VOG die niet ouder is dan één jaar. Opdrachtnemer geeft Opdrachtgever inzage in een VOG van een personeelslid, indien Opdrachtgever daarom vraagt. De VOG ziet in ieder geval op Categorie 1 (informatie) en categorie 4 (dienstverlening). Voor het overige personeel dat Opdrachtnemer inzet voor de uitvoering van de Opdracht is Opdrachtgever gerechtigd een verklaring van Opdrachtnemer te vorderen dat het door hem in te zetten personeel beschikt over een verklaring omtrent het gedrag (VOG), dat Opdrachtnemer daartoe de originele VOG('s) heeft opgevraagd en dat op het moment van de verklaring de VOG('s) niet ouder is/zijn dan een jaar, mits Opdrachtgever daarvan de noodzaak heeft aangetoond. Voorts dient Opdrachtnemer inzage te geven in een VOG van een personeelslid, indien Opdrachtgever daarom verzoekt en Opdrachtgever daarvan de noodzaak heeft aangetoond. Indien Opdrachtnemer gevestigd is in een andere lidstaat dan Nederland, dan dient voor "VOG" te worden gelezen: een bewijsmiddel uit het land van vestiging van Opdrachtnemer dat een aan de VOG gelijkwaardig doel dient. Indien Opdrachtnemer niet verklaart c.q. inzage geeft conform hetgeen Opdrachtgever heeft gevorderd, is Opdrachtgever gerechtigd te eisen dat het betreffende personeelslid niet (langer) voor de uitvoering van de Opdracht wordt ingezet.
E8.	Geheimhoudingsverklaring	Uw medewerkers ondertekenen voor de aanvang van de opdracht een geheimhoudingsverklaring dat alle informatie die zij tot zich krijgen in het kader van de opdracht, zij het bewust, zij het per ongeluk strikt geheim zullen houden richting eenieder die buiten het kader van de opdracht valt. Wij verstrekken deze geheimhoudingsverklaring.
E9.	Aanmaken gebruikersaccounts	Voor het aanmaken van gebruikersaccounts binnen onze omgeving, hebben wij de namen, initialen, e-mailadressen en geboortedata van uw medewerker(s) nodig. U verstrekt deze gegevens aan ons.
E10.	Voorwaarden voor gebruik	Uw medewerkers gebruiken onze middelen uitsluitend voor het uitvoeren van de opdracht. Elke vorm van gebruik voor derden of privégebruik is strikt verboden. Gebruik op een manier die ons kan schaden, of bij wet verboden is, is verboden.
E11.	Training & Awareness	Uw medewerkers zijn aantoonbaar getraind op veilig werken binnen een Citrix-platform en zich bewust van specifieke, en algemene informatiebeveiligingsrisico's.
E12.	Persoonsgebonden accounts	Het is uw werknemers expliciet verboden om accounts te delen. Elke medewerker dient zijn/ haar eigen account te gebruiken voor de toegang tot het Citrix-platform. Ook bij u intern mogen geen accounts gedeeld worden.
E13.	Werklocatie	Uw werknemers werken strikt vanuit een locatie welke binnen de Europese Unie valt. Uw werknemers werken niet op publieke locaties waar het voor anderen mogelijk is om mee te kijken op het scherm, mee te luisteren naar gesprekken, of mee te kijken naar het internetverkeer.

E14.	Security certificering	Gedurende de looptijd van de overeenkomst is de Opdrachtnemer ISO 27001-gecertificeerd met betrekking tot de scope van de Opdracht. Deze ISO 27001-certificering dient te zijn uitgevoerd door een geaccrediteerde certificeringsinstantie die erkend is door de Raad voor Accreditatie of een gelijkwaardig geaccrediteerd orgaan in het buitenland. De Opdrachtnemer dient tevens een actuele Statement of Applicability (SoA) aan te leveren, waarin duidelijk wordt uiteengezet welke beveiligingsmaatregelen van toepassing zijn en hoe deze worden geïmplementeerd. Deze SoA dient te worden ondersteund door een recent auditrapport van een ISO 27001-audit, uitgevoerd door een erkende, geaccrediteerde certificeringsinstantie (nationaal of internationaal). Indien de Opdrachtnemer niet ISO 27001-gecertificeerd is, kan een kwaliteitshandboek worden overgelegd waarin alle onderdelen van de ISO 27001-norm zijn uitgewerkt. Een externe, door een erkende instantie geaccrediteerde auditor dient te hebben vastgesteld dat de opgenomen PDCA-cyclus (Plan-Do-Check-Act) gelijkwaardig is aan de opzet zoals voorgeschreven door ISO 27001. Als alternatief voor een ISO 27001-certificering kan een ISAE 3000- of ISAE 3402-assurancerapportage worden overlegd, of een SOC 2- of SOC 3-assurancerapportage, uitgevoerd door een gekwalificeerde Certified Public Accountant (CPA) of accountantsorganisatie, conform de AICPA- en ISAE-normen en specifiek gericht op informatiebeveiliging of interne beheersing. De rapportage mag niet ouder zijn dan 12 maanden.
E15.	NIS2-richtlijn	De Universiteit Utrecht valt onder de verplichtingen van de NIS2-richtlijn. U waarborgt dat uw dienstverlening voldoet aan de eisen die onder NIS2-richtlijn kunnen vallen. Dit omvat onder andere risicomanagement, cybersecuritymaatregelen en incidentmelding. Op basis van de NIS2-richtlijn kunnen wij aanvullende eisen stellen en deze opnemen in de contractuele afspraken. Eventuele redelijke kosten die hiermee gepaard gaan, kunt u bij ons in rekening brengen. U gaat hiermee akkoord.
E16.	informatie-beveiligingsaudit	Opdrachtgever heeft het recht om voor de geleverde dienst een informatiebeveiligingsaudit te (laten) doen op het Citrix-platform, de systemen die Opdrachtnemer inzet bij de uitvoering van de opdracht en de omgang met gegevens van de Opdrachtgever. Inschrijver verleent kosteloos en zonder voorbehoud volledige medewerking aan een dergelijke audit en verstrekt volledig inzage in alle door de auditor documenten, bronnen, gegevensdragers, bestanden e.d.
E17.	Two-factor authenticatie	Uw interne systemen die onze informatie verwerken vereisen een two-factor authenticatie voordat gebruikers hier toegang tot krijgen.
E18.	Periodieke controle van (toegangs)rechten	U controleert en rapporteert regelmatig (minimaal eenmaal per zes (6) maanden) of al uw medewerkers nog over de juiste rechten beschikken. Dit doet u ook als er iemand van rol wisselt of uw bedrijf verlaat. Indien de rechten niet meer passend zijn past u dit gelijk aan. Als wij hiervoor rechten in moeten trekken laat u ons dit onmiddellijk weten.
E19.	Beveiliging hulpsystemen	Hulpsystemen zijn systemen die u gebruikt om de opdracht uit te kunnen voeren. Denk aan communicatiesystemen, systemen voor samenwerking, monitoringsystemen, en systemen voor dataopslag.

		De hulpsystemen die ingezet worden door u dienen adequaat beveiligd te zijn: inzage of wijziging van gegevens door daartoe ongeautoriseerde gebruikers moet onmogelijk zijn en gebruik van de systemen door daartoe ongeautoriseerde gebruikers moet onmogelijk zijn. U kunt dit op verzoek van ons aantonen.
E20.	Wachtwoordkluis	Indien geheimen (accountgegevens, wachtwoorden, SSH-keys, API-keys etc) aan u overgedragen worden, dan dient u deze op te slaan in een versleutelde wachtwoordkluis. Aangezien deze gegevens uniek zijn per medewerker, moet elke medewerker die over deze gegevens beschikt een eigen, met uniek wachtwoord beveiligde, wachtwoordkluis hebben om deze gegevens in te bewaren.
E21.	Beveiligde verbindingen en koppelingen	Alle koppelvlakken waarop informatie uitgewisseld wordt met andere informatiesystemen dienen door u gedocumenteerd te zijn en passende beveiliging te kennen tegen misbruik. Koppelvlakken die gegevens uitwisselen dienen versleutelde transportmiddelen te gebruiken. Pogingen tot ongeautoriseerde toegang en geautoriseerde toegang en wijzigingen dienen gelogd te worden. Praktisch betekent dit: • Firewalls op netwerk- en host-niveau dienen computersystemen af te schermen; • Database-koppelingen over netwerkinfrastructuur moeten versleuteld zijn; • Authenticatie-koppelingen over netwerk infrastructuur moeten versleuteld zijn; • Ongebruikte koppelvlakken (o.a. databasepoorten, beheerinterfaces, web services) dienen uitgeschakeld te zijn; • Transport van gegevens gaat (daar waar mogelijk) versleuteld. • Moderne TLS standaarden dienen gevolgd te worden (zie NCSC publicatie); • Systemen worden gecompartmenteerd volgens het zoneringsmodel van de Opdrachtgever; • Informatiebeveiligingsrichtlijnen van de Opdrachtgever worden geïmplementeerd.
E22.	Veilige werkplekken	U dient alle endpoints (waaronder laptops, desktops, mobiele apparaten en servers) die toegang hebben tot systemen of gegevens van Opdrachtgever actueel, ondersteund en beveiligd te houden. Besturingssystemen, software, firmware, beveiligingspatches en malwaredefinities moeten tijdig worden bijgewerkt, waarbij kritieke beveiligingsupdates zo spoedig mogelijk en overige beveiligingsupdates uiterlijk binnen 30 dagen na beschikbaarstelling moeten zijn geïmplementeerd. Endpoints met achterstallige beveiligingsupdates, niet-ondersteunde software of uitgeschakelde beveiligingsvoorzieningen mogen geen toegang hebben tot gevoelige of kritieke gegevens. Alle endpoints moeten zijn voorzien van actuele en centraal beheerde antimalwarebescherming en beveiligd zijn met sterke authenticatie, waaronder minimaal een individueel account en een wachtwoordbeleid conform actuele beveiligingsstandaarden.

F. Privacy

Nr.	Onderwerp	Eis
F1.	P1 Data Transfer Impact Assessments	Opdrachtnemer heeft een Data Transfer Impact Assessments (DTIA) uitgevoerd voor de start van de uitvoering, indien voor de uitvoering van de Opdracht persoonsgegevens zullen worden doorgegeven aan een derde land of een internationale organisatie (in de zin van de AVG) door de Opdrachtnemer, tenzij doorgifte aan een derde land of een internationale organisatie plaatsvindt waarvan de Europese Commissie heeft bepaald dat het een passend beschermingsniveau waarborgt. Op verzoek van Opdrachtgever deelt Opdrachtnemer deze DTIA met Opdrachtgever.
F2.	P2 DPIAs	Opdrachtnemer verleent volledige medewerking, waaronder het verstrekken van alle relevante informatie, aan Opdrachtgever teneinde Opdrachtgever in voorkomend geval in staat te stellen een Data Protection Impact Assessment (DPIA) conform art. 35 AVG uit te voeren en uiterlijk binnen drie maanden na gunning van de Opdracht af te ronden. Indien uit deze DPIA blijkt dat (additionele) technische of organisatorische beveiligingsmaatregelen moeten worden genomen teneinde de vastgestelde risico's te mitigeren, dan zal Opdrachtnemer alle medewerking verlenen om deze technische en/of organisatorische beveiligingsmaatregelen te treffen (waaronder inbegrepen technische en/of organisatorische beveiligingsmaatregelen die bij de Opdrachtnemer moeten worden genomen). Eventuele kosten die hieraan verbonden (kunnen) zijn aan de zijde van Opdrachtnemer - voor medewerking aan de DPIA en het implementeren van technische en/of organisatorische beveiligingsmaatregelen, komen voor rekening van Opdrachtnemer. In overleg kan daarvan worden afgeweken.
F3.	P3 Privacyverklaring	Opdrachtnemer verleent volledige medewerking aan Opdrachtgever om Opdrachtgever in voorkomend geval in staat te stellen een privacyverklaring op te stellen en te publiceren conform artt. 12, 13 en 14 AVG.
F4.	P4 Inbreuk in verband met persoonsgegevens	Opdrachtnemer, of een dienstverlener van Opdrachtnemer, heeft de kennis, technische mogelijkheden (waaronder onder meer loggegevens) en procedures, om een inbreuk in verband met persoonsgegevens die worden verwerkt op grond van de verwerkersovereenkomst, tijdig vast te stellen, te onderzoeken en te beheersen.
F5.	P5 Verantwoordelijkheid	Opdrachtnemer heeft de verdeling van de rollen, taken en verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens op grond van de verwerkersovereenkomst in zijn organisatie schriftelijk vastgelegd en vastgesteld.
F6.	P6 Bewaartermijnen	Opdrachtnemer hanteert de door Opdrachtgever vastgestelde bewaartermijnen voor (categorieën van) persoonsgegevens die conform de verwerkersovereenkomst worden verwerkt en garandeert dat het verwijderen van persoonsgegevens uitvoerbaar is.
F7.	P7 Doelbinding	In lijn met de verwerkersovereenkomst verwerkt Opdrachtnemer persoonsgegevens uitsluitend op basis van schriftelijke instructies van Opdrachtgever en voor doeleinden die rechtstreeks voortvloeien uit de werkzaamheden die Partijen zijn overeengekomen, en zal Opdrachtnemer de persoonsgegevens in ieder geval niet gebruiken voor: • het uitvoeren van testen; en • het uitvoeren van data-analyses. Tenzij uitdrukkelijk en schriftelijk toestemming van de Opdrachtgever.

		In het geval dat persoonsgegevens moeten worden verwerkt voor het functioneren en de veiligheid (bijv. het tegengaan van ongewenste toegang door derden) van het Citrix-platform, garandeert de opdrachtnemer dat deze persoonsgegevens strikt noodzakelijk zijn voor deze doeleinden en dat de persoonsgegevens worden verwijderd wanneer ze niet meer noodzakelijk zijn (waaronder begrepen door de Opdrachtnemer geïmplementeerde technische updates waardoor de verwerking van persoonsgegevens niet meer noodzakelijk is).
--	--	---

G. Financieel

Nr.	Onderwerp	Eis
G1.	Financieel	De kosten voor beheerwerkzaamheden, de SLA, uw servicedesk en eventuele licentiekosten – voor zover deze licenties niet door ons worden verstrekt – zijn opgenomen in de maandelijksse beheerkosten. U hanteert een all-in tarief voor de beheerkosten. De beheerkosten betreffen de gehele scope van de opdracht, dus onder meer alle eisen in dit Programma van Eisen (tenzij expliciet anders aangegeven), inclusief hetgeen u heeft aangeboden bij de wensen, maar met uitzondering van de transitiekosten (zie voor de transitiekosten Eis G6). Deze beheerkosten zijn verschuldigd vanaf het moment van overdracht van het beheer (gepland op 11 oktober 2027, zie eis D2). Als het moment van overdracht later plaatsvindt dan 11 oktober 2027, dan verschuift automatisch het moment waarop wij de beheerkosten aan u verschuldigd zijn. U bent niet gerechtigd om tarieven in rekening te brengen anders dan de tarieven die u op grond van dit Programma van Eisen en de overeenkomst mag berekenen.
G2.	Financieel	U hanteert voor de inzet van een consultant, architect, projectmanager en engineer de vaste uurtarieven, zoals aangeboden in uw inschrijving.
G3.	Financieel	De door u ingediende prijzen/ tarieven zijn in euro's en exclusief de van toepassing zijnde btw-tarieven.
G4.	Financieel	De beheerkosten in het prijzenblad staan vast tot 1 januari 2029. Het overeengekomen tarief mag vervolgens eenmaal per jaar per 1 januari (voor het eerst per 1 januari 2029) worden aangepast naar aanleiding van indexatie en mag vanaf het desbetreffende jaar in rekening worden gebracht. Indexatie vindt plaats conform de CBS-tabel Dienstenprijzen; commerciële dienstverlening en transport, index 2021=100, regel 6202 Computeradviesing. Deze index is momenteel te bereiken via deze link: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/85817NED/table?dl=AC7CD. Voor het indexeren wordt uitgegaan van de jaar-op-jaarmethode waarbij het eerste kwartaal van voorgaand contractjaar de peildatum is. De maximale procentuele tariefswijziging is het percentage dat staat in de kolom Jaarmutaties, bij het derde kwartaal van het vorige kalenderjaar. Dus: voor de indexering van 2029 wordt gekeken naar de jaarmutatie bij het derde kwartaal van 2028.

		Indien de indexcijfers nog niet vastgesteld zijn, mogen de voorlopige cijfers gehanteerd worden zonder dat een eventuele verrekening achteraf plaats vindt. Een verzoek tot prijswijziging(en) dient u uiterlijk twee maanden voor 1 januari schriftelijk in te dienen bij de contract- en leveranciersmanager van de Universiteit Utrecht. U dient het voorstel (inclusief nieuwe prijslijsten) gespecificeerd met een uitdraai van CBS-Statline in. Ook maakt u in het voorstel een verwijzing naar de betreffende overeenkomst met de Universiteit Utrecht. Wij geven uitsluitend schriftelijk aan of wij akkoord gaan met het door u ingediende voorstel tot tariefwijziging. Na akkoord gaat de indexering in.
G5.	Financieel	De uurtarieven van de rollen in eis G2, zoals aangeboden in het prijzenblad staan vast tot 1 januari 2029. De overeengekomen uurtarieven mogen vervolgens eenmaal per jaar per 1 januari (voor het eerst per 1 januari 2029) worden aangepast naar aanleiding van indexatie. Indexatie vindt plaats conform de het CBS Cao-lonen, contractuele loonkosten en arbeidsduur; indexcijfers (2020=100, categorie J-Informatie en Communicatie (of bij wijziging van het basisjaar tijdens de contractduur het meest recente basisjaar). Hierbij worden de indexcijfers genomen van "Cao-lonen per uur incl. bijz. beloningen" van "Totaal Cao-sectoren". Deze index is (op dit moment) te bereiken via deze link: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/85663NED/table?dl=AC7D5. Voor het indexeren wordt uitgegaan van de jaar-op-jaarmethode waarbij het derde kwartaal van voorgaand contractjaar de peildatum is. De maximale procentuele tariefswijziging is het percentage dat staat in de kolom "Ontwikkeling t.o.v. een jaar eerder", bij het derde kwartaal van het vorige kalenderjaar. Dus: voor de indexering van 2029 wordt gekeken naar de jaarmutatatie bij het derde kwartaal van 2028. Indien de indexcijfers nog niet vastgesteld zijn, mogen de voorlopige cijfers gehanteerd worden zonder dat een eventuele verrekening achteraf plaats vindt. Een verzoek tot prijswijziging(en) dient u uiterlijk twee maanden voor 1 januari schriftelijk in te dienen bij de contract- en leveranciersmanager van de Universiteit Utrecht. U dient het voorstel (inclusief nieuwe prijslijsten) gespecificeerd met een uitdraai van CBS-Statline in. Ook maakt u in het voorstel een verwijzing naar de betreffende overeenkomst met de Universiteit Utrecht. Wij geven uitsluitend schriftelijk aan of wij akkoord gaan met het door u ingediende voorstel tot tariefwijziging.
G6.	Financieel	U hanteert een all-in tarief voor de transitiekosten. Deze transitiekosten betreffen de gehele transitie, zoals beschreven in het transitieplan. De transitiekosten betreffen alle kosten tot overdracht van het beheer (11 oktober 2027), inclusief de kosten voor het beheer van de omgevingen vóór overdracht, personele kosten, de licentiekosten – voor zover deze licenties niet door ons worden verstrekt –,kosten voor de OTAP-omgevingen vóór overdracht livegang en de door u aangeboden opleidings-/ trainingsprogramma's. Ook de kosten voor de nazorg tijdens een eventuele nazorgfase ná overdracht maken onderdeel uit van de transitiekosten.

G7.	Financieel	U hanteert onderstaande mijlpalen ten behoeve van de facturatie van de transitiekosten. Iedere mijlpaal wordt voorzien van een opleverdocument. Een mijlpaal is afgerond na acceptatie daarvan door ons. Pas na afronding van een mijlpaal mag u factureren. • Door ons goedgekeurd transitieplan (50%). • Succesvol afgeronde transitie, inclusief acceptatie door ons (50%).
G8.	Financieel	Betalingen die voorafgaand aan de acceptatie van de transitie of andere onderdelen van de opdracht worden verricht, vinden steeds plaats onder de opschortende voorwaarde van deze acceptatie.
G9.	Financieel	Als wij (door)ontwikkelingen wensen, die specifiek voor ons worden gemaakt en die expliciet niet onder de transitiekosten of de beheerkosten vallen, kunt u deze uitsluitend uitvoeren en in rekening brengen na onze schriftelijke goedkeuring van uw offerte. In deze offerte biedt u de uurtarieven aan, zoals aangeboden in uw inschrijving.
G10.	Financieel	U conformeert zich aan de verplichting dat wanneer wij in de toekomst nieuwe technologieën of dienstverlening, anders dan verbetering van bestaande modules of technologieën, willen afnemen (zoals modules en nieuwe technologieën die op het moment van inschrijven nog niet bestaan of nog niet uitvoerbaar zijn), u hier marktconforme prijzen voor offreert. De condities zoals beschreven in het Programma van Eisen en de offerteaanvraag betreffende de prijsstelling zijn geheel van toepassing op deze nieuw te offereen technologieën/ dienstverlening. De in de inschrijving aangeboden uurtarieven, conform het Prijzenblad, zijn hierbij van toepassing.
G11.	Financieel	Op ons verzoek biedt u opleidings-/ trainingsprogramma's aan buiten de transitiefase. Bijvoorbeeld voor het in gebruik nemen van nieuwe technologieën. U rekent hier marktconforme tarieven voor.

H. Facturatie

Nr.	Onderwerp	Eis
H1.	Facturatie	Bestellingen bevatten een bestelnummer (PO-nummer). U accepteert alleen bestellingen die zijn voorzien van een bestelnummer.
H2.	Facturatie	De beheerkosten factureert u éénmaal per maand. Meerwerk factureert u na acceptatie van het meerwerk door ons.
H3.	Facturatie	Facturen dienen te voldoen aan de factuurvereisten: Informatie voor leveranciers - Organisatie - Universiteit Utrecht (uu.nl). (Hyperlink = https://www.uu.nl/organisatie/praktische-zaken/informatie-voor-leveranciers/facturatie). Deze eisen kunnen gedurende de looptijd van de overeenkomst wijzigen. U moet dit zelf in de gaten houden.
H4.	Facturatie	Wij zijn aangesloten bij het PEPOL Acces Point. U verstuurt uw facturen als E-facturen. U levert E-facturen (inclusief bijlagen) aan volgens de werkwijze die staat op Informatie voor leveranciers - Organisatie - Universiteit Utrecht (uu.nl). (Hyperlink = https://www.uu.nl/organisatie/praktische-zaken/informatie-voor-leveranciers/facturatie). Deze eisen kunnen gedurende de looptijd van de overeenkomst wijzigen. U moet dit zelf in de gaten houden.

H5.	Facturatie	De Opdrachtgever beschikt momenteel over een SAP SRM bestelsysteem. De Opdrachtgever heeft echter een nieuw ERP-systeem (SAP4HANA) aangeschaft. De "Go-live" van het nieuwe ERP-systeem staat gepland in de eerste week van januari 2028. Het doel is een efficiënt "Bestellen tot Betalen proces" en een effectieve samenwerking met u als Opdrachtnemer. Het bijbehorende platform voor samenwerking met opdrachtnemers is het SAP Business Network. Hier vindt uitwisseling van digitale zakelijke documenten plaats, zoals inkooporders en orderbevestigingen. Op verzoek van Opdrachtgever zal Opdrachtnemer meewerken aan het ontvangen van orders en het geven van orderbevestigingen via het SAP Business Network.
------------	------------	--